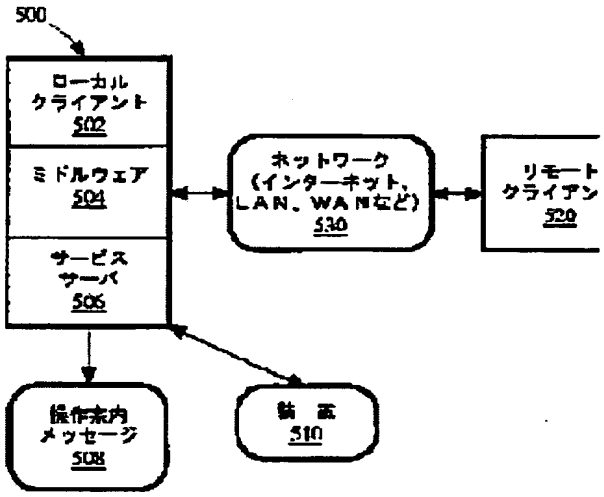
COMMUNICATION SYSTEM BETWEEN SERVICE SERVER AND SERVICE CLIENT

Japanese Patent No. 3224784

Patent number: JP11296595
Publication date: 1999-10-29
Inventor: YOOKU SHION CHIN
Applicant: INTERNATL BUSINESS MACH CORP <IBM>
Classification:
- international: G06F17/60; G06F13/00; G06F19/00
- european:
Application number: JP19990005704 19990112
Priority number(s):

Abstract of **JP11296595**

PROBLEM TO BE SOLVED: To easily adapt the communication system, including the service server and service client, to alterations of devices and services. SOLUTION: Service specifications issued for the service server 506 are defined on the basis of service specification models as to all services provided in a network 530. The service specification models define the framework of semantics for modeling the message format and flow between the server 506 and clients 502, 520 which are developed independently. This method includes a step for incorporating a client context token into a service request, a step for generating a service server event which can includes an exchange token, a step for regenerating a client context token in the service server event, and a step for generating a no-send request service server even which can include the exchange token.



(19)日本国特許庁（ＪＰ）　(12)特　許　公　報（Ｂ２）　(11)特許番号
特許第3224784号
(P3224784)
(45)発行日　平成13年11月５日(2001.11.5)　(24)登録日　平成13年８月24日(2001.8.24)

(51)Int.Cl.'	識別記号	FI	
G06F 17/60	324	G06F 17/60	324
	410		410A
	502		502
	ZEC		ZEC
13/00	357	13/00	357Z

請求項の数４(全 25 頁)

(21)出願番号　特願平11－5704
(22)出願日　平成11年１月12日(1999.1.12)
(65)公開番号　特開平11－296595
(43)公開日　平成11年10月29日(1999.10.29)
審査請求日　平成11年７月29日(1999.7.29)
(31)優先権主張番号　９８００１３２－４
(32)優先日　平成10年１月17日(1998.1.17)
(33)優先権主張国　シンガポール（ＳＧ）

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
〔INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(72)発明者　ヨーク・シオン・チン
シンガポール436885　タンジョン・ルー・ロード　６シー　ナンバー02－02
(74)代理人　100065455
弁理士　山本　仁朗　（外２名）

審査官　岩間　直純

最終頁に続く

(54)【発明の名称】　ネットワーク内のサービス・サーバと少なくとも１つのサービス・クライアントの間で通信する方法及びシステム

(57)【特許請求の範囲】
【請求項１】ネットワーク内のサービス・サーバと少なくとも１つのサービス・クライアントの間で通信する方法であって、
前記ネットワーク内のサービス・サーバ用のサービス仕様モデルに準拠して定義された前記サービス・サーバのサービス仕様を発行するステップと、
前記サービス仕様モデルに準拠して定義されたサービス要求を前記サービス・クライアントによって提出するステップと、
前記サービス要求に応答して前記サービス仕様モデルに準拠して定義された送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成するか、または非送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成するステップとを含み、

前記生成するステップが、前記送信請求サービス・サーバ・イベントまたは前記非送信請求サービス・サーバ・イベント内に引き換えクーポンを組み込むステップを含み、
前記引き換えクーポンが、サービス要求を受け入れるための前提条件が満たされているかどうかを前記サービス・サーバが後で判定するための前記サービス・サーバからの情報を含む、前記方法。
【請求項２】前記送信請求サービス・サーバ・イベントに応答して前記サービス・クライアントが前記引き換えクーポンを含む別のサービス要求を提出するステップをさらに含む、請求項１に記載の方法。
【請求項３】ネットワーク内のサービス・サーバと少なくとも１つのサービス・クライアントの間で通信するためのシステムであって、

前記ネットワーク内のサービス・サーバ用のサービス仕様モデルに準拠して定義された前記サービス・サーバのサービス仕様を発行する手段と、
前記サービス仕様モデルに準拠して定義されたサービス要求を前記サービス・クライアントによって提出する手段と、
前記サービス要求に応答して前記サービス仕様モデルに準拠して定義された送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成するか、または非送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成する手段とを備え、
前記生成する手段が、前記送信請求サービス・サーバ・イベントまたは前記非送信請求サービス・サーバ・イベント内に引き換えクーポンを組み込む手段を含み、
前記引き換えクーポンが、サービス要求を受け入れるための前提条件が満たされているかどうかを前記サービス・サーバが後で判定するための前記サービス・サーバからの情報とを含む、前記システム。
【請求項４】前記サーバ・イベントに応答して前記サービス・クライアントが前記引き換えクーポンを含む別のサービス要求を提出する手段をさらに備える、請求項３に記載のシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は公衆ネットワーク内の独立に開発されたサービス・サーバと１つまたは複数の独立に開発されたサービス・クライアントの間の通信、特にサービス・サーバのサービスを定義して発行し、サービス・クライアントからのサービス要求の結果を要求して取得し、サービス・サーバがイベントをサービス・クライアントに個別に通知するための方法、装置、およびシステムに関する。
【０００２】
【従来の技術】いくつかの従来のホスト・コンピュータおよび端末構成を図１および図２に示す。同図では各ホスト・コンピュータが１つまたは複数の端末と通信する。ホスト・コンピュータ・アプリケーション・ソフトウェアへのオンライン・アクセスは、キーボード（図示せず）およびディスプレイ・モニタを備えた端末１１２の使用から始まった。端末１１２には、ホスト処理コンピュータ１１０宛のまたはそこからのメッセージとタンデム接続された端末装置が動作するための定義済みの固定論理がインストールされている。端末コンピュータ１１２はホスト・コンピュータ１１０の入出力端末として用いられる。
【０００３】関連するホスト・コンピュータの例としては、ＵＮＩＸベースのコンピュータおよびメインフレームが含まれる。このようなシステムでは、ホスト・コンピュータ１２０、１３０とリモート端末１２２、１３２との間のメッセージは、所定のフォーマットおよびフロー（例えばそれぞれＡＳＣＩＩキーストロークとＩＢＭ３２７０データストリームおよびフロー）に準拠することが必要とされる。ホスト・コンピュータ１２０、１３０は端末１２２、１３２のキーボードからの入力を受信して端末１２２、１３２のディスプレイ・モニタへ出力を送信する。
【０００４】いくつかのビジネス環境では端末１４２、１５２として他の装置、例えば現金自動支払機、通帳プリンタなどを使用することも必要とされる。例えば、銀行のメインフレーム１４０は、現金自動支払機などの非標準装置を備えた自動預金支払機（ＡＴＭ）１４２に接続できる。従来から、このような非標準または特殊装置は制御装置のコンピュータにインストールされているソフトウェアによって直接制御されている。このソフトウェアは特殊装置が提供する直接インターフェースに関してプログラムされている。ネットワーク環境では、装置コントローラ・ソフトウェアは通常クライアント・ソフトウェアへのサーバとして動作する。この場合、メインフレーム１４０とＡＴＭ１４２の間の通信は、例えばＩＢＭ３６２４、ＩＢＭ４７３Ｘ、Ｄｉｅｂｏｌｄ９１２、またはＮＣＲ　ＡＴＭのメッセージ・フォーマットおよびフローを介して実行できる。あるいは、銀行の制御装置１５０を、通帳プリンタ１５２など別の非標準装置を備えたブランチテラー・パーソナル・コンピュータ（ＰＣ）に接続することもできる。この構成はまたソフトウェア固有のメッセージ・フォーマットおよびフローを必要とする。したがって、特別のメッセージ・フォーマットおよびフローがこれらの端末１４２、１５２用に定義される。
【０００５】この場合、端末キーボードからの入力に加えて、ホスト・コンピュータ１４０、１５０は通帳プリンタやカード読取装置などのいくつかの非標準装置からの入力を受信することができる。同様に、端末のディスプレイ装置に加えて、ホスト・コンピュータ１４０、１５０はレシート・プリンタ、現金自動支払機などの非標準装置へ出力を送信する。このように、しばしば極めて特殊なデータストリームやフローを必要とする多数の可能な端末装置が一般に利用される。
【０００６】さらに、ホスト・コンピュータと端末のこのような構成には、インターネットおよびイントラネットのためのウェブ・サーバ１６０およびブラウザ・コンピュータ１６２が含まれる。その場合、多様なブラウザ・アプリケーションを用いてＰＣからウェブ・サーバにアクセスすることができる。ブラウザＰＣはｈｔｔｐメッセージを介してウェブ・サーバ用の入出力端末として動作する。
【０００７】要するに、図１および図２に示すシステムのメッセージ・フォーマットおよびフローは、ホスト・コンピュータ・アプリケーションが端末１２２、１３２、１４２、１５２、１６２内の装置から入力を受信し

そこへ出力を送信することができるように定義される。したがって、メッセージ・フォーマットおよびフローは各端末の装置の個々の選択と各装置の特性に極めて特有である。例えば、ホスト・コンピュータは、ＡＴＭの非標準装置に前もって挿入されている銀行カードなどの磁気ストライプ上に符号化される、磁気トラック・データを含むフィールドを備えたメッセージを送信することができる。

【０００８】このようなホスト・コンピュータおよび端末の既存のメッセージ・フォーマットおよびフローは、新しい装置が端末で使用できるようになったとき、それをサポートするためにしばしば拡張しなければならない。このように、メッセージ・フォーマットおよびフローは多様で複雑なだけでなく、新しい端末装置に適応しなければならないことが多い。

【０００９】また、メッセージ・フォーマットは、人間のユーザおよびメッセージのソースを認証するためのフィールドを含むこともできる。例えば、これらのフィールドは、暗号化された個人識別番号（ＰＩＮ）およびメッセージ認証ダイジェストをそれぞれ必要とすることがある。メッセージ・フォーマット内のこのようなフィールドは、メッセージの違法な盗聴および改竄を防止するためにオンライン・アクセスが機密である場合に必要になることがある。

【００１０】複数の組織にまたがって端末コンピュータを共用するために、メッセージを図３に示すような組織間のホスト・コンピュータのために定義できる。これらのメッセージも、ネットワーク２０４、２１４、２２４の端末、それぞれの端末ネットワークのホスト処理コンピュータ２０２、２１２、２２２、および他の組織のホスト・コンピュータ（例えばＡＮＳＩ　Ｘ９．２）の間で分散される定義された機能に特有である。

【００１１】組織間ホスト・コンピュータ・メッセージは他の組織（例えば電子資金転送用のＳＷＩＦＴ）へのサービス提供のためにも定義できる。このようなシステムの例を図４に示す。図では、ホスト処理コンピュータ３０２、３１２、３２２が相互の通信用に構成されている。このような組織間メッセージは装置依存ではなく、組織間データ（例えば資金）転送の目的に特有である。例えば、いくつかの大手の製造業者および小売業者はデータを交換するために用いる標準化データ・フォーマットである電子データ交換（ＥＤＩ）を用いる。

【００１２】端末がより強力になり処理能力が増すにつれて、サーバとしてパッケージ化されたより多くの機能を提供し、従来のメインフレーム・コンピュータまたは別のコンピュータに常駐するクライアントへサービスを提供する。クライアント・サーバ技術の進歩により、サーバ機能は直接装置動作のレベルにある必要がなく、複数の装置または装置あたり複数の動作を含むより高次のレベルにあってもよいようになっている。このことは、

かなりの処理能力を備えたホスト・コンピュータであるクライアントおよびサーバ・コンピュータでは自明である。

【００１３】この状況は、サービス要求元（すなわち「クライアント」）およびサービス・サーバの動作が極めて特殊なメッセージ・フォーマットおよびフローにより密結合された状況である。メッセージ・フォーマットおよびフローは、サーバが提供しようとするサービスに特有である。例えば、サービス要求元すなわちクライアントは、図２の銀行のメインフレーム・コンピュータ・アプリケーション１４０であり、サービス・サーバはＡＴＭ１４２の内蔵ソフトウェアであり、銀行のメインフレーム・アプリケーションがＡＴＭの現金自動支払機のサービスを要求する。

【００１４】サービス要求元とサービス・サーバの間のメッセージのフローおよびフォーマットは通信レイヤとは別個に定義される。さらに、メッセージは同じコンピュータ上で走っているクライアントとサーバの間を流れることもできる。例えば、メッセージはアプリケーション・プログラム・インターフェース（ＡＰＩ）呼出しまたはローカル・ソケット・メッセージを介することもできる。提供されるサービスが変わるとき、クライアント側およびサーバ側のソフトウェアの同期状態を維持するためにこれらを同時に更新する必要がある場合が極めて多い。

【００１５】クライアントには、そのクライアントがサーバによって提供されたサービス・セットを使用するための認証を受けた期限内のみこのサービス・セットへのアクセスが提供される。サービス呼出しのシーケンスもサービスの性質およびサービスの提供方法と密に結合していることがある。例えば、トランザクション状況メッセージは、端末でのトランザクション実行のためのトランザクション許可がホスト・コンピュータから受信された後で初めて、端末からホスト・コンピュータへ送信できる。

【００１６】簡素な管理用ワークステーションに寄せる企業の関心から、アプリケーション・サーバからアプリケーション（例えばウェブ・ページ、Ｊａｖａアプレット）をロードしてサーバ上でアプリケーションを実行するネットワーク・コンピュータが生まれた。そのようなネットワーク・コンピュータは、サーバ上で実行されるＷｉｎｄｏｗｓアプリケーションのためのリモート・ユーザ・インターフェースを提供する。明確なＰＣ構成は、アプリケーション・サーバとは別個に実行できる。しかしこの手法はＰＣに接続される非標準装置に対応できない。

【００１７】

【発明が解決しようとする課題】本発明の目的は、サービス・サーバおよびサービス・クライアントを含む通信システムにおいて装置やサービスの変更に容易に対応で

きるようにすることにある。

【００１８】

【課題を解決するための手段】本発明の第１の態様によれば、ネットワーク内のサービス・サーバと少なくとも１つのサービス・クライアントの間で通信する方法であって、ネットワーク内のサービス・サーバ用のサービス仕様モデルに準拠して定義された、サービス・サーバのサービス仕様を発行するステップと、前記サービス仕様モデルに準拠して定義されたサービス要求を前記サービス・クライアントによって提出するステップと、前記サービス仕様モデルに準拠して定義されたサービス・サーバ・イベントを前記サービス・サーバによって生成するステップとを含む通信方法が提供される。

【００１９】サービス仕様モデルは、互いに独立に開発されたサービス・サーバとサービス・クライアントの間のメッセージ・フォーマットおよびフローをモデル化するためのセマンティクスの枠組みを定義することが好ましい。

【００２０】この方法は、クライアント・コンテキスト・トークンをサービス要求に組み込むステップをも含むことが好ましい。またこの方法は、サービス要求に応答して送信請求サービス・サーバ・イベントをサービス・サーバによって生成するステップ、または非送信請求サービス・サーバ・イベントを前記サービス・サーバによって生成するステップを含むことができる。さらに、この方法は、送信請求サービス・サーバ・イベント内のクライアント・コンテキスト・トークンを再生するステップを含むこともできる。

【００２１】この方法は、送信請求サービス・サーバ・イベントまたは非送信請求サービス・サーバ・イベント内に引き換えクーポンを組み込むステップを含むことが好ましい。引き換えクーポンは、サービス要求を別のサービス要求に関連づける、送信請求サービス・サーバ・イベントからの情報を含む。引き換えクーポンは、別のサービス要求を受け入れるための１つまたは複数の前提条件が満たされているかどうかをサービス・サーバが後で判定するためのサービス・サーバからの情報を含むことができる。オプションで、１つまたは複数の前提条件は、一組のサービス・サーバ・イベントと、１つまたは複数の以前のサービス・サーバ・イベントからの累計マイレージ・ポイントとからなるグループのうち少なくとも１つを含む。ただし、サービス・サーバによる前記別のサービス要求の受け入れが生ずるのは、サービス・クライアントのために前者の一組のサービス・サーバ・イベントのうち少なくとも１つが事前に生起している場合である。また、後者の累計マイレージ・ポイントは、サービス・サーバがその裁量でリセットできる。すなわち、引き換えクーポンとは、サービス・サーバによって提供される情報を含む、サーバ・コンテキスト・トークンを表すものである。この情報により、サービス・サーバは、サービス要求のコンテキストを判定し、このコンテキストが累積した価値（例えば、累計マイレージ・ポイント）を判定し、その完全性を検査することができる。累積した価値が一定値に達すると、サービス・クライアントは、それに見合った何らかの権利に引き換えることができる。

【００２２】この方法は、サーバ・イベントに応答してサービス・クライアントが引き換えクーポンを含む別のサービス要求を提出するステップをさらに含むことが好ましい。サービス・サーバは、別のサービス要求の引き換えクーポンを用いて別のサービス要求を処理するクライアント・コンテキストを決定することができる。

【００２３】オプションとして、この方法は、サービス・サーバで実行されるステップとして、サポートされるサービスおよびサービス・サーバの対応するサービス仕様に関してサービス要求を確認（validate）するステップと、サービス・クライアントを確認または認証するステップと、引き換えクーポンを含むサービス・サーバ要求メッセージを確認または認証するステップとからなるグループのうちの少なくとも１つをさらに含むことができる。また、サービス・クライアントによるこの方法の実行は、オプションとして、サービス・クライアントがサービス・サーバ・イベントを確認するステップと、サービス・サーバを確認または認証するステップと、クライアント・コンテキスト・トークンを確認または認証するステップとからなるグループのうち少なくとも１つを含むことができる。

【００２４】オプションとして、サービス・クライアントは、サービス・サーバを実装するコンピュータ・システム内で実装される。これはコンピュータ・システムにダウンロードされコンピュータ・システムによって実行されるアプリケーション・ソフトウェアを用いて行うことができる。

【００２５】本発明の第２の態様によれば、ネットワーク内のサービス・サーバと少なくとも１つのサービス・クライアントの間で通信するためのシステムであって、ネットワーク内のサービス・サーバ用のサービス仕様モデルに準拠して定義された、サービス・サーバのサービス仕様を発行する手段と、サービス仕様モデルに準拠して定義されたサービス要求をサービス・クライアントによって提出する手段と、前記サービス仕様モデルに準拠して定義されたサービス・サーバ・イベントを前記サービス・サーバによって生成する手段とを備えるシステムが提供される。

【００２６】

【００２７】

【発明の実施の形態】本発明は、ネットワーク化された環境内のサービス・サーバが提供するサービスを定義し、発行し、サービス要求の結果を要求して取得し、サービス・サーバ・イベントの非同期の非送信請求通知を

行う方法、装置およびシステムに関する。本発明の好ましい実施形態は、ネットワーク化された環境の独立に開発されたサービス・クライアントとサービス・サーバの間のメッセージ・フォーマットおよびフローを、サービス・クライアントおよびサービス・サーバ・ソフトウェアの開発者の間での最小限の同期調整によって効率よくモデル化できる、簡単な仕様のセマンティクスの一般的な枠組みを提供する。これは、サービス・サーバの既存のサービスを阻害することなく新しいサービスの導入を可能にし、またネットワーク・コンピュータのオープンで柔軟な構成の基礎を形成するのに使用され得る。個々のサービスはダウンロードされたクライアント・ソフトウェア（例えばＪａｖａアプレット、ＡｃｔｉｖｅＸオブジェクトなど）またはリモート・コンピュータで実行されるアプリケーションであり、ネットワーク・コンピュータの構成はキーボード、ディスプレイ、マウス、スマート・カード読取装置などの標準装置に限定されない。好ましい実施形態で開発される手法は、各サービス・サーバがそのサービス仕様を独立に定義して発行することに基づいている。これらの仕様は、管理組織によって管理されないコンピュータの動作を構成するのに使用されるデータの基礎を形成することができる。例えば、この仕様はローカルのスマート・カード・チップまたはリモート・コンピュータからロードできる。好ましい実施形態のシステムは、メッセージ・フォーマットおよびフローを定義しない。メッセージ・フォーマットおよびフローの実際の定義は、サービス仕様およびそのイベント・シーケンスに直接に準拠しているか、またはそれらにマップする。

【００２８】ネットワーク化環境の概要

ネットワークに接続されたどのコンピュータも本発明の好ましい実施形態に従って公衆ネットワーク内の他の任意のコンピュータ（すなわちサービス・クライアント）に対してサービス・サーバとして動作できる環境を図５に示す。このネットワーク化環境の例では、ＡＴＭ４２０およびキオスク４２２が設置され、公衆ネットワーク４００、好ましくはインターネットまたはイントラネットを介してサービス局４１８によって適用される。サービス局４１８は、そのキオスクのサービスを複数の異なる加入者組織の消費者に提供する。加入者組織はキオスクとの間で用いる専用のアプリケーション・ソフトウェアを独立に開発して維持する。アプリケーション・ソフトウェアは、加入者のウェブ・サイトを介して提供されるＷＷＷアプリケーションでもよい。この例のサービス局４１８はＡＴＭに現金を補給し、必要があればいつでもＡＴＭを修理する責任がある。銀行４２８などの加入者組織の顧客はＡＴＭ４２０から現金を取得することができる。さらに、旅行代理店４３２など他の加入者組織の顧客もキオスク４２２を使って旅行のチケットを購入できる。

【００２９】サービス局４１８自体が、消費者がキオスクを操作する手助けをする過程で消費者のためにキオスク装置を操作するサービス要求を出すコール・センタ・エージェントを有することができる。このシナリオでは、サービス局４１８が適用するコンピュータによって実施されるキオスク・ネットワーク・マネジャは、ＡＴＭ４２０およびキオスク４２２へのサービス要求元（クライアント）である。キオスク・ネットワーク・マネジャはこれらの端末４２０、４２２へコマンドを送信し、共通処理状況応答（例えばキー同期コマンド）を取得する。ネットワーク・マネジャはまた端末から非送信請求端末状況変更通知を取得する。

【００３０】銀行４１０は、ブランチ・ローカル・エリア・ネットワーク（ＬＡＮ）４２４、そのテラーＰＣ、および接続されたテラー装置（例えば通帳プリンタなど）を所有する。ブランチＬＡＮ４２４、テラーＰＣ、および接続されたテラー装置は、銀行４１０、および例えば銀行４１０が買収したばかりの銀行４２８の両方の顧客へサービスを提供する。

【００３１】スタチュトリ・ボード（statutory board）４２６は、そのサービス・クライアントである輸出入会社４１２へ公衆ネットワーク４００を介して関税処理サービスも提供するサービス・サーバとして動作できる。

【００３２】ホームＰＣ４３０は、ホームＰＣ４３０へのサービス・サーバである銀行４１０からＰＣオペレータの口座残高に基づいて購入クーポンを取得するサービス・クライアントでもよい。購入クーポンはホリデイ・パッケージを購入するために公衆ネットワーク４００を介して、サービス・サーバとして機能する旅行代理店４３２へ渡される。クーポンはその後サービス・クライアントとして機能する旅行代理店４３２によって適切な資金を引き出すために銀行４１０へ提出される。

【００３３】キオスク４２２は銀行４２８のウェブ・サイトからウェブ・ページを取り出すこともできる。ウェブ・ページは銀行４２８の顧客サービスの一環として銀行４２８のためにキオスク４２２上でローカルに実行可能なＪａｖａアプレットを備えることができる。

【００３４】ネットワーク・コンピュータ４１６は、アプリケーション・サーバ４１４からアプリケーション・ソフトウェア（例えばＷＷＷページおよびＪａｖａアプレット）をロードして実行し、サーバ４１４が実行するＷｉｎｄｏｗｓアプリケーションのためのリモート・ユーザ・インターフェースを提供することができる。キーボード、マウス、ディスプレイ・モニタ、スマート・カード読取装置などの標準ＰＣ装置に加えて、通帳プリンタを含むその他の非標準装置もネットワーク・コンピュータ４１６に接続することができる。

【００３５】前述のネットワーク化環境の例から理解できるように、多数のさまざまな加入者組織、コンピュー

タ・システム，および非標準装置が公衆ネットワークを介して利用できる。ネットワークに接続されたコンポーネントはそれぞれ他のコンポーネントおよびそれ自体に対してサービス・サーバとしてもサービス・クライアントとしても動作できる。各コンポーネントは専用のメッセージ・フォーマットおよびフローを有することができるため，このようなコンポーネントを使用するクライアントおよびサーバ・ソフトウェアの設計者には可能な組み合わせが無数に存在するという点で重要な課題が課せられている。

【００３６】以上のように，公衆ネットワーク環境は，サービス・サーバを利用しようとする個々の組織が開発するクライアント・ソフトウェアの個々の開発者にとって，本出願人が識別した幾多の困難を提起する。

【００３７】上記のネットワーク環境が提起する１つの困難は，サービス・クライアントのために個別に開発されたソフトウェアがどの特定のサービス・サーバにもサービスを要求する方法である。クライアント・ソフトウェアの個々の開発者が開発および試験の基準とする，明確で簡素で曖昧でないサービス仕様モデルが必要である。サービスの定義も異種ネットワーク間で有効であるためにはネットワーク・トランスポートおよびネットワーク・プロトコルから独立している必要がある。この課題に対処するための一般の手法は，サービスおよび各サービスを使用するのに必要な固有のメッセージ・フォーマットおよびシーケンスを発行することである。例えば，ＡＴＭの供給業者はその装置に固有のメッセージ・フォーマットおよびフローを提供できる。しかしながら，これにはクライアント・ソフトウェアが各装置に固有の多様なメッセージ・フォーマットおよびフローに対応できることが必要である。サービス・サーバ・ソフトウェアはまた合意された規格に従って，サービス問い合わせメッセージに応答してサービス機能のディスカバリに参加したり，サービス機能公示メッセージを生成したりすることもできる。

【００３８】ネットワーク化された環境における別の困難は，サービス・クライアント用の独立に開発されたソフトウェアがサービス・サーバが用いる仕様を満足することをサービス・サーバが検証できなければならないことである。

【００３９】さらに別の困難は，クライアント・ソフトウェアによるサービスの「違法な」使用（例えば，消費者がカードを挿入する前にＰＩＮ入力を要求したり，あるいはサービス・サーバ内のデータベースへの違法な更新を要求する）をどう防止するかである。サービスをできる限り適法である（例えば，リモート・アプリケーションによって実行できないオペレーションへサービスを提供しない）よう定義できる一方で，ある種の「機密」サービスは依然として認証されたサービス・クライアントだけに提供しなければならない。サービス要求は，以前にサービス・サーバによって生成されまだ「満了」していない一組のサービス・サーバ・イベントの直後に行われるならば，サービス・サーバによって受け入れられる。これには次の例がある。

（ａ）現金支払サービス要求は，所定の条件を満たすサービス・クライアントからのみ許される。その条件とは，サービス・クライアントが認証されていて，以前に暗号化ＰＩＮ入力サービスを成功裏に要求しただけでなく，現金支払要求を受け付ける前にキオスクがタイムアウトにならず且つトランザクションを取り消していないことも必要とする。

（ｂ）ＰＩＮ入力を求めるサービス要求は，カードが先にキオスクに挿入されサービス要求がカードの妥当性検査のためにホスト・コンピュータへ送信された場合に限って，サービス・クライアントとして動作するホスト・コンピュータから受け入れられる。

【００４０】さらに，サービス・サーバが承認された一定の方式で動作するようにできることが必要である。例えば，キオスクで消費者のカードを返却する過程で同じプロンプトが表示され，同じタイムアウト時に消費者はどのサービス・クライアントがサービスの対象であるかにかかわらず同じ消費者対話操作を用いて，カードを確保する前に再度指示される。また，クライアントがカードを（例えばトランザクションを取り消すために）イジェクトできないようにし，なおかつ後でキオスクから現金を引き出せるようにする必要がある。

【００４１】さらに別の困難は，各クライアントがサービス・サーバから同時にサービスを受けているサービス要求の複数のスレッドを有し得ることである。各スレッドのサービス要求は相互に関連している。したがって，好ましい実施形態では，サービス・サーバは新しいサービス要求を同じコンテキストに対するものとして以前のサービス要求に関連付けることができなければならない。新しいコンテキストはサービス・サーバ・イベントで開始する。サービス・サーバ・イベントに応答して実行されるサービス要求は，イベントが属するコンテキストの一部である。後続のサービス・サーバ・イベントも同じコンテキストの一部となることができる。

【００４２】さらなる困難は，サービス・クライアントが，サービス・サーバからの送信請求サービス・サーバ・イベントを，先にサービス・サーバへ送出されたサーバ要求に応答して生成されるものとして関連付けることができなければならないことである。

【００４３】別の困難は，所与のコンテキストに対する以前のサービス要求の完了前に，同じサービス・クライアントからの新しいサービス要求を受け入れることができるということである。例えば，これはサービス・クライアントが以前に出したサービス要求の処理を取り消す，同じクライアントからのサービス要求を含む。

【００４４】さらに，安全でないネットワークでは，サ

ービス・サーバがサービス・クライアントの識別を認証でき、サービス・クライアントがサービス・サーバの識別を認証でき、サービス・サーバが引き換えクーポンを含むサービス要求メッセージを認証でき、サービス・クライアントがクライアント・コンテキスト・トークンを含むサービス・サーバ・イベント・メッセージを認証でき、サービス・クライアントおよびサービス・サーバがサービス・クライアントとサービス・サーバの間で転送されるデータの選択された部分を暗号化できる必要がある。サービス・サーバの所有者およびサービス・クライアントの所有者は、アプリケーションの機密保護要件によって、また要求される機密保護策がすでに他の手段（例えばミドルウェア、イントラネット・ファイアウォール）を介して利用できるかどうかによって、上記の機密保護機能の全部または一部が不要であると決定できる。

【００４５】最後に、サービス・サーバがサービス要求をどう処理するかについてのサービス・クライアントの予想が、サービス・サーバが実際にサポートする内容と一致することをサービス・サーバが確認する必要がある。

【００４６】本発明の好ましい実施形態はこれらの困難を克服できるか少なくとも緩和できるサービス仕様を提供する。

【００４７】好ましい実施形態のサービス・サーバとサービス・クライアント好ましい実施形態によれば、サービス・サーバは装置（例え現金自動支払機、カード読取装置、キーボードなど）のいかなる動作に関するサービスも提供できる。また、サービス・サーバはオプションで人間の対話操作を必要とし、そのサービスの提供時に案内メッセージの使用を要する。例えば、メインフレーム・コンピュータ上で走るアプリケーションは、サービスの提供時に人間の対話操作を必要としないサービス・サーバの１つの形式である。これとは対照的に、サービス・サーバとして動作するキオスク（例えば図５の４２２）は、消費者との対話（例えば消費者にキオスクの現金自動支払機４２０から現金を取り出すよう依頼すること）を必要とするサービス・クライアントとして動作するバックエンドのメインフレーム・アプリケーションが要求するサービスを提供できる。キオスクが提供するサービスがサービス・サーバ側で人間の対話操作を含むこの状況では、キオスク装置を含むサービス・オペレーションは案内画面またはメッセージと連携して行われる必要がある。

【００４８】好ましい実施形態によるこのようなサービス・サーバは、サービス・クライアントからのサービス要求に対して1つまたは複数のサービス・サーバ・イベントで応答する。これは装置の非同期動作とネットワークを介して提供される応答メッセージの非同期的な性質に対応する。サービスの実行またはパフォーマンスで複数のイベントが生成されることがある。したがって、イベントは単一の、複数の、または反復するイベントである。例えば、サービス要求の処理は、それぞれをクライアントがイベントによって通知される必要がある複数のステップを含むことがある。サービスの実行は反復するイベントも生成することがある。例えば、キオスクがあるサービス・クライアントについて銀行カード、クレジット・カードその他を受け入れられるようにするサービス要求は、クライアントの顧客によってカードが新たに挿入されるたびに１つのイベントを生成する。

【００４９】さらに、サービス・サーバに事前登録された（すなわちオフライン）サービス・クライアントは、サービス・サーバから非送信請求サービス・サーバ・イベントを受信することもできる。例えば、サービス・サーバとして動作するブラウザＰＣは、サービス・クライアントとして動作するＷＷＷサイトにウェブ・ページをブラウザＰＣへ送信させる非送信請求サービス・サーバ・イベント（例えばＨＴＴＰ　ＧＥＴ）を送信できる。ＨＴＴＰ　ＧＥＴ応答は、ウェブ・ページおよび送信請求入力の提示を求めるブラウザへのサービス要求を表す。ウェブ・サイトまたはサーバは、それ自体を、サービス・クライアントとして動作するブラウザＰＣからサービス要求（例えばＨＴＴＰ　ＧＥＴ）を受信するサービス・サーバとみなすこともできる。これは、１対のサービス・サーバが相互動作し、個別に他方をサービス・クライアントと見なす、数多くの可能性の１例である。Ｊａｖａアプレットを含むクライアント・ソフトウェアは、サービス・サーバ・コンピュータで実行するためにダウンロードできる。この場合メッセージはローカルであり、おそらくはプロセス間またはスレッド間メッセージである。

【００５０】サービス要求およびサービス・サーバ・イベントと共に可変およびコンテキスト依存の情報を提供するデータ要素が引き渡される。これらのデータ要素は、実行可能スクリプト、例えば署名が必要なことがあるＪａｖａアプレット、Ｊａｖａ　Ｓｃｒｉｐｔ、ＨＴＭＬを運ぶことができる。

【００５１】図６に好ましい実施形態によるサービス・サーバと１つまたは複数のサービス・クライアントを示す。サービス・サーバ５０６は、ＡＴＭなどの端末５００を用いて実施できる。端末５００はまた、ネットワーク通信のためのミドルウェア５０４とオプションとしてローカル・クライアント５０２を含むことができる。サービス・サーバ５０６は端末装置に操作案内メッセージ５０８を提供し、１つまたは複数の端末装置５１０の動作を制御する。サービス・サーバは端末装置を直接管理し制御する。この例では、リモート（サービス）・クライアント５２０はサービスに関してインターネット、イントラネット、ＬＡＮ、ワイド・エリア・ネットワーク（ＷＡＮ）などのネットワーク５３０で伝送されるメッ

セージを介してサービス・サーバ５０６と通信する。ローカル（サービス）・クライアント５０２はローカルにインストールされたクライアント・アプリケーションまたはリモート・コンピュータ要素（例えば５２０）からダウンロードされたアプリケーション（例えばＪａｖａアプレット）である。このようなローカル・クライアント５０２はメッセージまたはアプリケーション・プログラム・インターフェース（ＡＰＩ）呼出しを介してサービス・サーバ５０６と通信する。好ましい実施形態によるサービス仕様規格はクライアント－サーバ間通信のセマンティクスとして用いられ、ネットワーク中心のものである。これはサービス・クライアントとサービス・サーバの間のメッセージ・フォーマットおよびフローを特に定義しない。この図は好ましい実施形態のサービス仕様モデルが適用されるサービス・クライアント、サービス・サーバ、およびネットワーク化環境のブロック図である。

【００５２】サービス仕様モデル

以下のサービス仕様モデルは特定の好ましい実施形態の詳細を提供する。ただし、本発明は提示された特定の例に限定されるものではない。逆に、本発明の範囲と精神を逸脱しない限りで、当業者には明らかな修正または変更を本発明に加えることができる。ネットワークのサービス・サーバのサービス仕様を以下にサービス・サーバが提供するサービスごとに説明する。

【００５３】表Ａ、Ｂ、Ｃ、およびＤにサービス・サーバのサービス仕様を定義し、発行する方法を詳述する。

【００５４】表Ａ：サービス・サーバ仕様

（Ａ）サービス・サーバＩｄ：ユニコード名文字列。

（Ｂ）サーバ記述：これによってクライアントによる自動検出と潜在的なクライアントへの広告が可能になる。

（Ｃ）サービス要求メッセージ・タイプおよびサービス・サーバ・イベント・メッセージ・タイプの両方についてディジタル署名を生成するためにサービス・サーバがサポートするアルゴリズム・タイプ。この仕様はサービス・サーバが定義して発行するさまざまな可能なアルゴリズムに関する。これらのアルゴリズムは、さまざまな業界標準アルゴリズムと連携してメッセージ内容を用いるランダム・シーディングのさまざまな組み合わせを使ってメッセージに署名することができる。サービス要求メッセージ内のディジタル署名を生成するのに用いるメッセージ内容は、サービス要求メッセージ内のクライアントＩＤその他の機密メッセージ要素（例えば引き換えクーポン）を含む必要がある。サービス・サーバ・イベント・メッセージ内のディジタル署名を生成するのに用いるメッセージ内容は、サーバＩＤ、サービス要求メッセージからコピーされたクライアント・コンテキスト・トークン（送信請求サービス・サーバ・イベントの場合）、その他のサービス・サーバ・イベント・メッセージ内の機密メッセージ要素を含む必要がある。業界標準アルゴリズムの例は共通秘密対称鍵を用いるデータ暗号化標準（ＤＥＳ）およびディジタル証明書を用いるＲＳＡ公開鍵アルゴリズムである。

（Ｄ）サービス要求メッセージ・タイプおよびサービス・サーバ・イベント・メッセージ・タイプの両方の選択されたデータ要素の暗号化のためにサービス・サーバによってサポートされるアルゴリズム・タイプ。この仕様はサービス・サーバが定義して発行するさまざまな可能なアルゴリズムに関する。これらのアルゴリズムはサービス要求メッセージ内の選択されたデータ要素を暗号化するために用いる鍵をシードするサービス要求メッセージの一部として伝送されるランダム・データと、サービス・サーバ・イベント・メッセージ内の選択されたデータ要素を暗号化するためのサービス・サーバ・イベント・メッセージの一部として伝送されるランダム・データを用いることができる。業界標準アルゴリズムの例は共通秘密対称鍵を用いるデータ暗号化標準（ＤＥＳ）およびディジタル証明書を用いるＲＳＡ公開鍵アルゴリズムである。

【００５５】表Ｂ：サポートされた各サービス要求のサービス仕様

（Ａ）サービス要求識別仕様：ネットワークのサービス・サーバ内で一意的なユニコード・サービス名文字列。

（Ｂ）サービス要求カテゴリ識別仕様：ネットワークのサービス・サーバ内で一意的なユニコード・サービス名文字列。これによりサービス要求の分類が可能になる。

（Ｃ）下記のいずれかを含む前提サービス要求受け入れモードおよび条件。

ｉ）満足すべき１つまたは複数の前提セット：これはサービス要求への複数の経路を可能にする。セット内で、前提サーバ・イベントは複数回要求されることがある。前提セットの例は「（Ａ、Ｂ）、（Ａ２、Ｄ、Ｅ）、（Ｃ３）」、ただしＡ、Ｂ、Ｃ、Ｄ、Ｅはサーバ・イベントＩＤ／カテゴリの組み合わせである。第２のセットを用いる場合、サーバ・イベントＡは２回要求される。第３のセットを用いる場合、サーバ・イベントＣは３回発生する必要がある。引き換えクーポンは最後のＣイベントで戻される。

ｉｉ）最小累計イベント・ポイント：これらは以前のサーバ・イベントからの同じクライアントについての同じコンテキストで要求される。引き換えクーポンは十分なポイントに達した最後のイベントで戻される。

Ｄ）サービス要求がサービス・サーバからのサービス・サーバ・イベントとは別個にサービス・サーバへ提出できるかどうかに関するブール値。コンテキストの一部でないサービス要求（すなわちサービス・サーバ・イベントに応答しないサービス要求）はここでは真と指定される。この仕様が真の場合、次のリストが適用される。

ｉ）同時発生のサービス要求ＩＤ／カテゴリの組み合わせのリスト：このリストはサービス・サーバがこのサー

ビス要求の処理中に受け入れることができる同じクライアントからのサービス要求を識別するために提供される。例えば、このリストはこのサービス要求をその処理中に取り消すことができるサービス要求のＩＤ／カテゴリを含むことができる。

Ｅ）引き換えクーポンが必要かどうかを示すブール値。

Ｆ）データ引き数のリスト：各引き数はサービスが要求する特定の情報を提供し、「データＩＤ＝値」によって識別される。この仕様はまた提供されないすべての引き数のデフォルト値を示す。これらはクライアントまたはサーバの構成に拘束されないフリー・フォーマット仕様である。データ要素ごとに、データ要素を暗号化するかどうかについてのブール値が提供される。データ要素ごとにそのテキスト記述を設けておけば、自動検出にとって有用である。

Ｇ）送信請求サーバ・イベント情報：このサービス要求の処理の結果生成されるイベントのリストを含む。サービスが同期化されていてもその完了は少なくとも１つのイベントで示される。以下にリストするイベントは他のサービス要求の結果として生成できるイベントとしても指定できる。

ｉ）各イベントは一意的に識別される。サービス要求とその結果であるイベントとを容易に関連付けられるように、サービス要求ＩＤ／カテゴリ文字列の組み合わせはイベントＩＤ／カテゴリ文字列の組み合わせの一部とすることが推奨される。これはそのイベントが１つの特定のサービス要求だけの結果である場合に重要である。

ａ）サーバ・イベントＩＤユニコード文字列：各サーバ・イベント・カテゴリ内で一意的

ｂ）サーバ・イベント・カテゴリＩＤユニコード文字列：送信請求および非送信請求サーバ・イベント・カテゴリの両方についてサーバ内で一意的

ｉｉ）各イベントに関する詳細情報：

ａ）記述テキスト：自動検出に有用

ｂ）引き換えクーポンがこのイベント・メッセージで利用できるかどうかを示すブール値

ｃ）このイベントで得た累計マイレージ・ポイント（ある場合）

ｄ）記述テキストの記述：サーバの自動検出に有用

ｅ）サービス・サーバ・イベント・データ項目のリスト。各データ項目はイベントに関する特定の情報を提供し、「データＩＤ＝値」によって識別される。この仕様はデータ項目のフォーマットを指定しない。データ項目ごとに、ブール値がデータ項目を暗号化するかどうかを示す。データ要素ごとにそのテキスト記述を設けておくと、自動検出にとって有用である。

ｆ）次の４つの値を含むグループの１つからのフラグ：

－新しいコンテキストの開始

－コンテキストの中間

－コンテキストの終り、および

－コンテキストの一部ではないイベント外の値

ｇ）このイベントの受信時にサーバ・クライアントが発行できる１つまたは複数のサービス要求セットのリスト。例えば（（Ａ、Ｂ）、（Ｃ、Ｄ、Ｅ）、（Ｆ、Ｆ））はサービス要求Ａ、ＣまたはＦがこのイベントを受信するサービス・クライアントから受け入れられることを意味する。サービス要求Ａが処理されている間、サービス要求Ｂをサービス・サーバへ発行でき、サービス要求Ｃが処理されている間、サービス要求ＤまたはＥをサービス・サーバへ発行でき、サービス要求Ｆが処理されている間、別のサービス要求Ｆをサービス・サーバへ発行できる。

ｉｉｉ）ＩＤ文字列および所定の意味を有する標準イベント

ａ）サービス不明

ｂ）サービス仕様不一致

ｃ）コンテキストがサービス・サーバによって取り消されれた（例えば、消費者がＣＡＮＣＥＬキーを押下）

ｄ）コンテキストが同じクライアントからの受け入れられたサービス要求によって取り消された

ｅ）必要な資源（例えば装置）が利用できない

ｆ）引き換えクーポンが引き換え済み

ｇ）引き換えクーポンが無効

ｈ）引き換えクーポンが期限切れ

ｉ）クライアント認証失敗

ｊ）引き換えクーポン認証失敗

ｉｖ）未定義の理由による拒否を含む他の非標準イベント・タイプについての情報

ａ）再発しているかどうかに関するブール値

ｂ）イベントがサービス要求の処理の終了を示しているかどうかに関するブール値

【００５６】表Ｃ：サポートされている各非送信請求サービス・サーバ・イベントのサービス仕様

ｉ）各サーバ・イベント・カテゴリ内で一意的なサーバ・イベントＩＤ

ｉｉ）送信請求および非送信請求サービス・サーバ・イベント・カテゴリのサーバ内で一意的なサーバ・イベント・カテゴリ識別

ｉｉｉ）記述テキスト：自動検出に有用

ｉｖ）イベントに関する詳細情報

＊　引き換えクーポンがこのイベント・メッセージで利用できるかどうかに関するブール値

＊　このイベントで得た累計マイレージ・ポイント（ある場合）

＊　サービス・サーバ・イベント・データ項目のリスト。各データ項目はイベントに関する特定の情報を提供し、「データＩＤ＝値」によって識別される。この仕様はデータ項目のフォーマットを指定しない。データ項目ごとに、ブール値がデータ項目を暗号化するかどうかを示す。

＊　次の４つの値を含むグループの１つからのフラグ：新しいコンテキストの開始．コンテキストの中間．コンテキストの終り．およびコンテキストの一部ではないイベント外の値

＊　このイベントの受信時にサーバ・クライアントが発行できる１つまたは複数のサービス要求セットのリスト。（（Ａ、Ｂ）、（Ｃ．Ｄ、Ｅ）．（Ｆ、Ｆ））はサービス要求Ａ．ＣまたはＦがこのイベントを受信するサービス・クライアントから受け入れられることを意味する。サービス要求Ａが処理されている間、サービス要求Ｂをサービス・サーバへ発行でき、サービス要求Ｃが処理されている間．サービス要求ＤまたはＥをサービス・サーバへ発行でき、サービス要求Ｆが処理されている間．別のサービス要求Ｆを発行できる。

【００５７】表Ｄ：メッセージ・タイプおよび要素のサービス仕様

ｉ）サービス要求メッセージ仕様

ａ）サービス要求識別

ｂ）サービス要求カテゴリ識別

ｃ）データ引き数のリスト：各引き数はサービスが要求する特定の情報を提供する。各引き数は「データＩＤ＝値」によって識別される。

ｄ）サービス仕様概要：これによってサービス・サーバのソフトウェアはクライアントが用いるサービス仕様がサービス・サーバがサポートする内容と一致することを確認することができる。

ｅ）クライアントＩＤ

ｆ）クライアント・コンテキスト・トークン（生成された１つまたは複数のサーバ・イベント内でサーバによって再生される）

ｇ）クライアントのためにこのサービス要求が用いる引き換えクーポン。引き換えクーポンは現在のサービス要求がサービス・サーバが所望の状態（例えば以前のサービス要求に応答する１つまたは複数の以前のサービス・サーバ・イベントの生成）に到達した後で処理されることを確認するためにサービス・サーバが用いることができる。例えば．以前の鍵同期化要求の完了の成功．成功裏の消費者カードの受け入れおよびＰＩＮ入力の請求がある。サービス・サーバはまた引き換えクーポンが依然として有効であることを確認する。例えば、サービスがタイムアウトして最後のトランザクションを取り消すことがあり、またはサービス・サーバが再ブートした場合もある。引き換えクーポンには次の２つのソースがある。

＊　サービス・クライアントからの以前のサービス要求を処理する際に生成された１つまたは複数のサービス・サーバ・イベント。引き換えクーポンはクライアントからの以前のサービス要求への応答で生成されたサーバ・イベントで戻される。サービス要求がサービス・サーバ・イベントとは別個に発行されたために引き換えクーポンが利用できない場合、またはサービス要求に適じるサービス・サーバ・イベントが引き換えクーポンを提供しない場合には．この引き換えクーポンは空白である。

＊　クライアントへの以前の非送信請求サービス・サーバ・イベント。例えば、キオスクでのカード挿入の発生の結果、サービス・サーバ・イベントがカードの確認のためにホストへ送信される。このサービス・サーバ・イベントはホストがＰＩＮ入力を請求するためにキオスクへのサービス要求内で用いることができる。

ｈ）サービス・サーバがサービス要求メッセージ（すなわち上記の項目）を認証することを可能にする安全なディジタル署名を生成する際に用いるアルゴリズム・タイプ。サービス・クライアントが使用される認証アルゴリズムを示す。サービス・サーバは、このフィールドの使用が各サービス・クライアントにとって必須であるかどうかを指定され得る。各サービス・クライアントは安全でないネットワークの一部でもよいしそうでなくてもよい。

ｉ）選択されたデータ要素を暗号化する際に用いるアルゴリズム・タイプ。

ｊ）サービス要求メッセージそれ自体を認証する安全なディジタル署名。これによってサービス・サーバは次の動作が可能になる。

＊　ソース（すなわちクライアントＩＤ）の認証

＊　サービス要求の改ざん（例えばデータ要素の変更）の検出

＊　無許可のクライアントによる引き換えクーポンの違法な記録／再生の検出

ディジタル署名の詳細は定義されず．サービス・サーバの所有者の指定に任されている。署名はオプションである。管理が行き届いたイントラネットではこれは不要である。必要な認証はサービス・サーバ５０６とサービス・クライアント５０２、５２０を接続するミドルウェア５０４によっても提供される。サービス・サーバはこのフィールドの使用が各サービス・クライアントにとって必須であるかどうかを指定され得る。各サービス・クライアントは安全でないネットワークの一部でもよいしそうでなくてもよい。

ｋ）暗号化に用いる暗号化鍵のランダム・シード。これはサービス・クライアントおよびサービス・サーバの両方だけが知っている固定秘密鍵の下で暗号化されたランダム鍵でもよい。

ｉｉ）サービス・サーバ・イベント・メッセージ仕様

ａ）イベント・メッセージが送信請求されているかどうかを示すブール値

ｂ）イベントを起動するサービス要求の識別（非送信請求の場合は無視）

ｃ）イベントを起動するサービス要求カテゴリの識別

ｄ）サーバＩＤ

ｅ）サービス・サーバ・イベントＩＤ

ｆ）サービス・サーバ・イベント・カテゴリ
ｇ）クライアント・コンテキスト・クーポンのコピー（非送信請求の場合は無視）
ｈ）サービス・サーバ・イベント・データ項目のリスト：各項目はサービスが提供する特定情報を与える。各引き数は「データＩＤ＝値」によって識別される。
ｉ）サーバがディジタル署名を生成するのに用いるアルゴリズム・タイプ。サーバは使用する認証アルゴリズムを示す必要がある。
ｊ）上にリストしたサービス・サーバ・イベント・メッセージ内容を認証する安全なディジタル署名。これは任意選択である。管理が行き届いたイントラネットではこれは不要である。必要な認証はサーバとクライアントを接続するミドルウェアによっても提供される。これはサービス・クライアントとサービス・サーバ間のビジネス調整契約の一部として構成されるオプションである。
ｋ）選択されたデータ要素の暗号化に用いるアルゴリズム・タイプ
＊　送信請求の場合、サービス要求メッセージ内でクライアントによって指定される。
＊　非送信請求の場合、サービス・サーバ内で構成される。
ｌ）サービス・サーバ・イベント引き換えクーポン。この仕様はクーポンのフォーマットの発行を必要としない。ここにリストする詳細は例にすぎない。これはサービス仕様の一部ではないため、発行する必要がない。クライアントが知る必要があるのは次のサービス要求でこのクーポンを含む必要があるということである。提案される内容はサーバの裁量に任されている。
＊　次のような情報への参照用のコンテキストＩＤ：
－最後のサービス要求のＩＤ
－クーポンが対象とするサービス・クライアントのＩＤ
－同じクライアントについての同じコンテキストの前提サービス要求処理情報。これは例えば、現在のコンテキストについてクライアントのためにサーバによりこれまでの累計されたマイレージ・ポイント、または現在のコンテキストについてクライアントのマイレージを取得するために発生したサーバ・イベントのリストでよい。
＊　以前に生成された引き換えクーポンの再使用を防ぐために必要に応じてサービス・サーバによって日付／時間スタンプと共に生成される乱数。サービス・サーバはこの乱数を以降のサービス要求で用いるランダムに変化するパスワードとして使用できる。
＊　サービス・サーバがその裁量で一部または全部を暗号化できる。
ｍ）選択されたデータ要素の暗号化のために使用される暗号化鍵のランダム・シード。これはサービス・クライアントおよびサービス・サーバの両方だけが知っている固定秘密鍵の下で暗号化されたランダム鍵でもよい。

【００５８】好ましい実施形態によれば、サービスは図６に示す関連するサービス・サーバ５０６がサービス要求を処理する過程およびこのような処理の最後に必要とするすべての操作案内および対話を提供する。サービスを要求しているときはサービス・クライアント・ソフトウェア５０２．５２０は同時に操作案内および対話５０８を提供することはない。これによってサービス・サーバ５０６は人間のオペレータのために一貫した操作案内および対話５０８を保証することができる。以下のサービス仕様はサービスを提供する過程で必要なすべての操作案内および対話５０８がサービス内で提供されなくてはならないことを規定する。サービス提供の過程とサービス提供の最後に用いられる操作案内および対話５０８自体はサービス仕様の一部ではない。操作案内および対話５０８はＬＥＤによって提供され、ディスプレイ・モニタの表示のみによらなくてもよい。これはオプションであり、サービス・サーバ５０６の裁量に任される。したがって、サービス・サーバの所有者はサービス・クライアント・ソフトウェア５０２、５２０に影響を与えずに操作案内および対話５０８を変更できる。これはサービス・サーバ５０６が動作して操作案内および対話５０８を一貫して承認された方式で提供することを保証する手助けをする。サービス・サーバ５０６はディスプレイ案内および対話の目的を含むサービスを提供できる。実際の表示および対話はサービス・サーバの裁量に任されている。

【００５９】さらに、サービス・サーバ５０６はサービスの処理中に必要に応じて人間の案内を引き継ぐ能力を必要とする。例えば、サービス・サーバは現金を払い出して消費者に払い出された現金を受け取るよう促しながらクライアントのダウンロードされたＪａｖａアプレットやウェブ・ページからディスプレイ画面を引き継ぐ能力がなくてはならない。これはブラウザ・ウィンドウを最小化または非表示にするサービス・サーバによって達成できる。

【００６０】サービス仕様では、クライアントＩＤはサービス・サーバ５０６がサービス・クライアント５０２．５２０を識別するためにも必要である。同様に、クライアント５０２、５２０はサービス・サーバ５０６を識別するためにサーバＩＤを必要とする。クライアントＩＤおよびサーバＩＤは関連するサービスを提供するサービス・サーバ５０６が決定して割り当てることができる。サーバＩＤはクライアント５０２．５２０が識別できるある種のサブネット内では一意的である（例えば一意的なインターネット・ホストＩＰアドレス）。代替的に、一意的なクライアントＩＤおよびサーバＩＤはネットワーク機関が割り当てることもできる。サービス・サーバからサービスを利用する必要があるすべてのクライアント５０２．５２０はビジネス調整契約の一部として、クライアントＩＤ、サービス・サーバＩＤ、および認証または暗号化に必要な鍵をそれぞれ取得する必要が

ある。契約はオンラインでいかようにもして取得できる。同様に、クライアント／サーバＩＤは任意の方法でネットワーキング・トランスポート・アドレスにマッピングできる。これらは両方とも図６のネットワーキング・ミドルウェア５０４のドメインである。

【００６１】サービス仕様ではまたクライアント・コンテキスト・トークンはサービス・サーバ５０６へのサービス要求（例えば下記の図７ないし図９のサービス要求６０４を参照）の一部としてサービス・クライアント５０２．５２０が提出できる。サービス・サーバ５０６はサービス要求を処理することで生成される１つまたは複数のサービス・サーバ・イベント内でクライアント・コンテキスト・トークンを再生する。これによってサービス・クライアント５０２．５２０はサービス・サーバ・イベントを以前に提出したサービス要求へ関連付けることができる。サービス仕様はトークンの特定のフォーマットを定義しない。トークン・フォーマットはクライアントの私的定義に委ねられ．クライアントによって発行される必要がない。サービス・サーバ５０６が実行する必要があるのは．それをクライアントのサービス要求を処理した結果として生成される１つまたは複数のサーバ・イベントへ返すことである。クライアント・コンテキスト・トークンの認証はそれを発行したサービス・クライアント５０２．５２０の裁量に完全に任されている。例えば、サービス・クライアント５０２、５２０は暗号化技術（例えば動的トークン内容データをクライアントにだけ知られた秘密鍵とＸＯＲする）を用いてそのクライアント・コンテキスト・トークンの完全性を検査できる。クライアント・コンテキスト・トークンのフォーマットを定義しないことでサービス・クライアントがコンテキスト・トークンの正確さと完全性を自由に検証できるようにする。トークンは発行元によって有効期限切れにされる場合もある（例えばクライアントが応答サービス・サーバ・イベントを待つのを諦めた場合）。

【００６２】引き換えクーポンは２つの特定の目的にかなう。第１の目的は、サービス・サーバ５０６がサービス要求を他の関連するサービス要求（例えば同じトランザクション、同じクライアント）に関連させることを可能にするデータを、サービス・サーバ５０６がクーポン内に直接または参照により間接的に配置することを許可することである。第２の目的は、サービス・サーバ５０６がサービス要求を受け入れるための前提条件（例えば以前のサービス要求が首尾よく完了したこと）が揃っているかどうかを判定することを可能にするデータを、サービス・サーバ５０６が直接または参照により間接的に配置できることである。引き換えクーポンはサービス・サーバ５０６からのサービス・サーバ・イベントでサーバ・クライアント５０２．５２０へ渡される。次に引き換えクーポンはサービス・サーバ５０６への次に関連するサービス要求の一部として提出される。要求を処理するために用いるコンテキストは引き換えクーポンを検査することでサービス・サーバ５０６によって識別される。

【００６３】この仕様は引き換えクーポンのフォーマットを定義しない。引き換えクーポンのフォーマットはサービス・サーバ５０６の私的定義に委ねられ、サービス・サーバ５０６によって発行される必要がない。サービス・クライアント５０２．５２０が実行する必要があるのはそれをサービス・サーバ５０６への次のサービス要求に入れることである。引き換えクーポンの認証はそれを発行したサービス・サーバ５０６の裁量に完全に任されている。例えば、サービス・サーバは暗号化技術（例えば動的内容データをサービス・サーバにだけ知られた秘密鍵とＸＯＲする）を用いてそのクーポンの完全性を検査できる。引き換えクーポンのフォーマットを定義しないことでサービス・サーバ５０６が引き換えクーポンの正確さと完全性を自由に確認できるようにする。引き換えクーポンは発行元によって有効期限切れにされる場合もある（例えばサービス・サーバがクーポンの宛て先からの次のサービス要求を待つのを諦めてトランザクションを取り消す場合）。

【００６４】それぞれのサービス要求は、満たされると引き換えクーポンに反映される、受け入れの前提条件を規定する。したがって、引き換えクーポンは累積的であり．その後に生成されたそれぞれの引き換えクーポンは以前のクーポンが使われないとマイレージを累積する。サービス要求前提条件チェック処理は２つのモードで定義および発行できる。第１に、サービス・サーバ５０６はクライアントのために選択されたサービス・サーバ・イベントを生成できる。これで、サービス・クライアント５０２、５２０についての選択されたイベントが以前に発生したことを条件としてサービス要求を受け入ることが可能になる。これらのイベントはクライアント５０２．５２０からの以前の選択された１つまたは複数のサービス要求の適切な処理の結果でもよい。第２に．クライアントは以前のイベントで十分なポイントを累積している場合がある。累計ポイントは戻された引き換えクーポンを利用してサービス・サーバ５０６によって追跡される。引き換えクーポンのフォーマットはクライアント・アプリケーションの開発者へ指示を与えるためにサービス・サーバ５０６によって発行されてもよい。上記のクーポンの宛て先が得たマイレージはサービス・サーバ５０６によって引き換えクーポン内に表すことができる。サービス・クライアント５０２．５２０が稼いだマイレージはサービス・サーバ５０６の裁量でリセットされる。

【００６５】サービス仕様では、それぞれのサービス要求は専用のデータ要素セットで定義される。また．それぞれのサービス・サーバ・イベント（イベントＩＤ）も専用のデータ要素セットで定義される。データ要素は、

基本の共通基本定義の内容を超えて、サービス・サーバ５０６とそのクライアント５０２、５２０の間でのデータ転送を可能にする。サービス・クライアント５０２、５２０があるサービス・サーバからデータ（例えば購入クーポン）を取得し、それをサービス要求に入れて他のサービス・サーバへ渡す必要がある場合、データ要素はそれを行うための手段を提供する。ただしこの場合はデータ要素のフォーマットおよび内容に関して２つのサービス・サーバ間での特殊な調整（例えば２つのサーバ間での専用セキュリティ方式）が必要である。必要に応じて、データ要素の暗号化がサービス・サーバによってサービス仕様内で指定される。サービス・サーバ５０６は非送信請求サービス・サーバ・イベントを発行することによってサービス・クライアントへ新しい鍵（所定の鍵で暗号化された）を通知することができる。データ要素は実行可能なスクリプトを含めるために用いることができる。このようなデータ要素はディジタル署名の生成に含まれることが多い。

【００６６】サービス仕様では、ディジタル署名はサービス要求およびサーバ・イベント・メッセージの真正さを確認するのに用いられるのが好ましい。ディジタル署名はメッセージのソースを認証し、メッセージの変更を検出し、無許可のサービス・クライアントによる引き換えクーポンの無許可の違法な記録および再生を検出するのに用いられる。

【００６７】上述したように、サービス要求は結果として反復イベントを生むことがある。したがって、反復サービス・サーバ・イベント・メッセージが用いられる（例えば、サービス・クライアントからのカード・トランザクション・サービス要求に応答してカード挿入につき１つ）。サービス仕様の前提事項の同期化を保証するため、それぞれのサービス要求の処理の一部として、クライアントが前提とするサービス仕様はサービス・サーバが実際にサポートする内容と比較される。

【００６８】サービス仕様では、サービス・クライアント５０２、５２０はサービス・サーバ・イベントを待っている間に必要に応じてタイムアウトすると予想される。

【００６９】また、サービス仕様には装置またはその機能への直接の参照はない。例えば、ディスプレイ・サービスはサービス・サーバ５０６が許可する形でディスプレイ装置５１０を間接的に使用する。これによってサービス要求を実行するために用いる装置５１０の構成の選択の柔軟性がサービス・サーバ５０６に提供される。

【００７０】サービス仕様では、サービス・サーバ・イベントは物理的イベント（例えば消費者カードの挿入と取り出し）の発生後に初めて発生する。

【００７１】サービス仕様は、サービスを要求しサービス要求の処理の結果を取得するためのネットワーク・メッセージ・フォーマットおよびフローを定義しない。したがって、サービス・サーバ５０６とサービス・クライアント５０２、５２０の間に通信、ハンドシェーク、保証付き送達などを提供することはミドルウェア５０４に一任されている。例えば、サービス・サーバ・イベントはミドルウェアが選択した最適化ストラテジを用いてサービス・サーバ５０６からの非同期メッセージにより通信できる。

【００７２】上述したように、サービス・クライアント５０２（例えばダウンロードされたＪａｖａアプレット）はサービス・サーバ５０６と同じ端末またはコンピュータ内でローカルに実行できる。

【００７３】このように、サービス仕様はメッセージ交換要件の全範囲をカバーしている。しかしながら、他の実施態様ではオプションとしてサービス仕様のサブセットだけを実施することも可能である。例えば、ネットワークが安全な場合にはデータ要素のディジタル署名／暗号化を省略でき、ミドルウェア５０４がクライアントおよびサーバのルーティングおよび認証を行う場合にはクライアントＩＤおよびサーバＩＤを省略できる。

【００７４】通信シナリオの例

図７はサービス・クライアント５０２、５２０とサービス・サーバ５０６間の通信の１つのシナリオを示す流れ図である。繰り返すが、サービス・クライアント５０２は端末上で実行できるダウンロードされたアプレットでもよい。処理はサービス・クライアント５０２、５２０がサービス・サーバ５０６へサービス要求６０４を送信するステップ６０２で開始する。サービス要求６０４はクライアント・コンテキスト・トークン１を含む。サービス・サーバ５０６はステップ６０６でサービス要求６０４に応答する。ステップ６０６で、サービス要求６０４はサポートされるサービスおよび対応するサービス仕様に関して確認される。またクライアントも確認／認証され、引き換えクーポンを含むサービス要求メッセージも確認／認証される。サービス要求６０４が拒否されると、サービス・サーバ拒否イベント６０８がサービス・サーバ５０６からサービス・クライアント５０２、５２０へ送信される。サービス・サーバ拒否イベント６０８はクライアント・コンテキスト・トークン１を再生し、サービス・サーバ５０６の処理を終了する。そうでない場合、すなわちサービス要求がサービス・サーバ５０６によって受け入れられた場合、処理はステップ６１０に進む。ステップ６１０で、コンテキストがサービス要求６０４から取り出される。このステップで、必要に応じて操作案内および対話が提供され、端末装置に関して複数の非同期動作が実行される。サービス・サーバ５０６は次にサービス・クライアント５０２、５２０へサービス・サーバ・イベント（送信請求）６１２を送信する。サービス・サーバ・イベント６１２は引き換えクーポンＡを含み、クライアント・コンテキスト・トークン１を再生する。サービス・サーバ・イベント（送信請求）６

１２は単一イベント、複数イベント、または反復イベントである。サービス・クライアント５０２、５２０はサービス・サーバ・イベント６１２を受信すると、ステップ６１４でサーバＩＤおよびクライアント・コンテキスト・トークンを含むサービス・サーバ・イベント・メッセージを確認／認証し、さらなるサービス要求６１６をサービス・サーバ５０６へ送信する。このさらなるサービス要求６１６はクライアント・コンテキスト・トークン２を含み、引き換えクーポンＡを再生する。

【００７５】通信処理はステップ６０６および６１０にしたがって第１のサービス要求６０４のときと同様に続行する。

【００７６】図８にサービス・サーバ５０６とサービス・クライアント５０２、５２０間のメッセージ・シナリオの第２の例を示す。処理はサービス・サーバ５０６がサービス・クライアント５０２、５２０にサービス・サーバ・イベント６５４を送信するステップ６５２で開始する。サービス・サーバ・イベント（非送信請求）６５４は引き換えクーポンＢを含む。サービス・クライアント５０２、５２０がサービス・サーバ・イベント６５４を受信すると、サービス要求６５８がステップ６５６でサービス・サーバ５０６へ送信される。サービス要求６５８はクライアント・コンテキスト・トークン３を含み、引き換えクーポンＢを再生する。ステップ６６０で、サービス・サーバ５０６はサポートされるサービスおよび対応するサービス仕様に関してサービス要求を確認し、クライアントおよび引き換えクーポンを含むサービス要求メッセージを確認／認証する。サービス要求がサービス・サーバ５０６により拒否される場合、サービス・サーバ拒否イベント６６２がサービス・クライアント５０２、５２０へ送信され、サービス・クライアント５０２、５２０はクライアント・コンテキスト・トークン３を再生する。そうでない場合、サービス・サーバ５０６の処理はステップ６６４に進む。ステップ６６４で、コンテキストが取り出され、必要に応じて操作案内および対話と非同期動作が実行される。サービス・サーバ５０６は次にサービス・クライアント５０２、５２０へサービス・サーバ・イベント（送信請求）６６６を送信する。サービス・サーバ・イベント６６６は引き換えクーポンＣを含み、クライアント・コンテキスト・トークン３を再生する。サービス・クライアント５０２、５２０はサーバＩＤおよびクライアント・コンテキスト・トークンを含むサービス・サーバ・イベント・メッセージを確認／認証し、ステップ６６８でサービス・サーバ５０６へサービス要求６７０を送信する。このさらなるサービス要求６７０はクライアント・コンテキスト・トークン４を含み、引き換えクーポンＣを再生する。

【００７７】図９にサービス・サーバ５０６とサービス・クライアント５０２、５２０間のメッセージ・シナリオの第３の例を示す。サービス・サーバ５０６はステップ６７２でサービス・クライアントへ非送信請求サービス・サーバ・イベントを送信する。サービス・サーバ・イベント（非送信請求）６７４はサーバ状況メッセージ、障害通知メッセージなどで、引き換えクーポンを備えることができる。

【００７８】ミドルウェア５０４はメッセージの完全性、同期化、保証付きメッセージ送達などのために図７ないし図９のシナリオのメッセージの上にさらにメッセージを構築することができ、また同じ情報を異なるフォーマットで表すこともできる。

【００７９】サービス・サーバ内のサービス要求の処理図１０および図１１はサーバ５０６内のサービス要求の処理の例を示す流れ図である。処理はステップ７００で開始する。ステップ７０２で、次のサービス要求がクライアントまたは内部ジョブ待ち行列から取得される。後者の場合、内部待ち行列からの内部的に生成されたサービス要求が非送信請求サーバ・イベントを生成する。判断ブロック７０４で、クライアントが有効かどうかを判定するためのチェックがなされる。クライアントが有効でなければ、拒否イベントがステップ７０６で通知される。そうでない場合、処理は判断ブロック７０８に進む。判断ブロック７０８で、引き換えクーポンを含むサービス要求が有効か、また変更されていないか（すなわちソースが有効かなど）を判定するためのチェックがなされる。ディジタル署名があればここで使用される。判定の結果有効でなければ、拒否イベントがステップ７１０で通知される。そうでない場合、処理は判断ブロック７１２に進む。判断ブロック７１２で、引き換えクーポンが有効かどうかを判定するためのチェックがなされる。これはコンテキストＩＤの突き合わせ、同じコンテキストを有する別のサービス要求が処理中であるかどうかのチェックを含む。問題なければ、引き換えクーポンがそのサービス要求に許されるかどうかを判定するためのチェックがなされる。また前提条件が満たされているかどうかを判定するためのチェックもなされる。判定結果がノーであれば、処理はステップ７１４に進み、拒否イベントが通知される。さもなければ、処理はステップ７１６に進む。ステップ７１６で、サービス要求メッセージの残りが分解される。これはサービス要求データ要素の抽出、選択したデータ要素の非暗号化、およびクライアント・コンテキスト・トークンがあればその保存を含む。処理は次に判断ブロック７１８に進む。

【００８０】判断ブロック７１８で、サービス要求が既存のコンテキストの一部であるかどうかを判定するためのチェックがなされる。判定結果がイエスであれば、処理はステップ７２４に進む。ステップ７２４で、コンテキスト制御ブロックが取り出される。処理は次にステップ７２６に進む。そうでない場合、すなわち判断ブロック７１８がノーを返した場合、処理は判断ブロック７２０に進む。判断ブロック７２０で、必要な１つまたは複

数の資源が利用できるかどうかを判定するためのチェックがなされる。利用可能でなければ、処理はステップ７２２に進み、イベントが通知される。されなければ、処理はステップ７２６に進む。

【００８１】ステップ７２６で、サービス要求に固有の処理がサービス要求状態に関して実行される。操作案内および対話が必要に応じて提供される。処理は次に判断ブロック７２８に進む。判断ブロック７２８で、これが新しいコンテキストであるかどうかを判定するためのチェックがなされる。新しいコンテキストであれば、処理はステップ７３０に進む。ステップ７３０で、クーポンに対して新しいコンテキストＩＤが割り当てられ、新しいコンテキスト制御ブロックが作成される。処理は次に判断ブロック７３２に進む。そうでない場合、すなわち判断ブロック７２８がノーを返した場合、処理は判断ブロック７３２に進む。

【００８２】判断ブロック７３２で、クライアントのための引き換えクーポンがあるかどうかを判定するためのチェックがなされる。判定結果がノーであれば、処理はステップ７３６に進み、さもなければ、ステップ７３４に進む。ステップ７３４で、引き換えクーポンが作成される。処理は次にステップ７３６に進む。

【００８３】ステップ７３６でイベント・メッセージが組み立てられる。ステップ７３８で、サービス・サーバ・イベントが通知される。判断ブロック７４０で、そのサービス要求についての処理が終了したかどうかを判定するためのチェックがなされる。まだであれば、処理はステップ７２６に戻る。

【００８４】終了の場合は、処理は判断ブロック７４２に進む。判断ブロック７４２で、コンテキストの終りまで到達したかどうかを判定するためのチェックがなされる。判定結果がイエスであれば、処理はステップ７４４に進む。ステップ７４４で、コンテキスト制御ブロックが削除される。処理は次にステップ７４６に進む。コンテキストの終りに達していなければ、処理はステップ７４８に進む。ステップ７４８で、コンテキスト制御ブロックが保存される。処理は次にステップ７４６に進む。ステップ７４６で、サービス要求の処理は終了する。

【００８５】サービス・クライアントでのサービス・サーバ・イベントの処理

図１２はサービス・クライアントでのサービス・サーバ・イベントの処理の例を示す流れ図である。処理はステップ８００で開始する。ステップ８０２で、次のサービス・サーバ・イベントがサービス・サーバから取得される。判断ブロック８０４で、サービス・サーバが有効かどうかを判定するためのチェックがなされる。サービス・サーバが有効でなければ、エラー処理がステップ８０６で実行される。さもなければ、処理は判断ブロック８０８に進む。判断ブロック８０８で、サーバ・イベントが有効かどうかを判定するためのチェックがなされる。このチェックはクライアント・コンテキスト・トークンを含むイベント・メッセージが有効か、また変更されていないか、ソースが認証されているかなどを判定するためのチェックを含む。ディジタル署名があればここで使用される。判定結果がノーであれば、エラー処理がステップ８１０で実行される。さもなければ、処理は判断ブロック８１２に進む。

【００８６】判断ブロック８１２で、サービス・サーバ・イベントが非送信請求かどうかを判定するためのチェックがなされる。非送信請求であれば、処理は判断ブロック８１６に進み、さもなければステップ８１４に進む。ステップ８１４で、コンテキストがクライアント・コンテキスト・トークンを用いて取り出される。処理は次に判断ブロック８１６に進む。

【００８７】判断ブロック８１６で、引き換えクーポンが利用可能かどうかを判定するためのチェックがなされる。すなわち、サービス・クライアントがサービス・サーバで以降の引き換えに利用できるクーポンがあるかどうかを判定するためのチェックがなされる。利用可能であれば、処理はステップ８１８に進む。ステップ８１８で、引き換えクーポンが後で使用するために保存される。処理は次にステップ８２０に進む。引き換えクーポンが利用可能でなければ、処理はステップ８２０に進む。ステップ８２０で、イベントが処理される。これはイベント・データ要素の抽出とそれから選択した要素の非暗号化を含む。処理は次に判断ブロック８２２に進む。

【００８８】判断ブロック８２２で、次のサービス要求をサービス・サーバへ出すかどうかを判定するためのチェックがなされる。出さないのであれば、処理は判断ブロック８２６に進み、さもなければステップ８２４に進む。ステップ８２４で、新しいクライアント・コンテキスト・トークンが作成され、サービス要求がサービス・サーバへ送られる。これはクライアント・コンテキスト・トークンの生成、データ要素の組立て（選択したデータ要素の暗号化を含む）、以前に保存された引き換えクーポンの取得、およびディジタル署名の構築を含み得る。処理は次に判断ブロック８２６に進む。

【００８９】判断ブロック８２６で、サービス・サーバ・イベントが非送信請求かどうかを判定するためのチェックがなされる。非送信請求であれば、処理はステップ８３０に進み、さもなければステップ８２８に進む。ステップ８２８で、処理されたサービス・サーバ・イベントに関連付けられていた既存のクライアント・コンテキストが削除され、処理は次にステップ８３０に進む。ステップ８３０でイベントの処理は終了する。

【００９０】

【００９１】

【図面の簡単な説明】

【図１】いくつかの従来のホスト・コンピュータおよび

31

端末構成を示すブロック図である。

【図２】いくつかの従来のホスト・コンピュータおよび端末構成を示すブロック図である。

【図３】それぞれ関連する端末ネットワークを備えたいくつかのホスト・コンピュータ間の通信を示すブロック図である。

【図４】いくつかのホスト・コンピュータ間での組織間通信を示すブロック図である。

【図５】本発明の好ましい実施形態によるサービス・サーバとサービス・クライアントの間の通信を可能にする公衆ネットワークを示すブロック図である。

【図６】好ましい実施形態によるネットワークのサービス・サーバとリモート・クライアントを示すブロック図である。

32

＊【図７】第１のシナリオの図６のサービス・サーバとサービス・クライアントの間のメッセージ伝送を示す流れ図である。

【図８】第２のシナリオのメッセージ伝送を示す流れ図である。

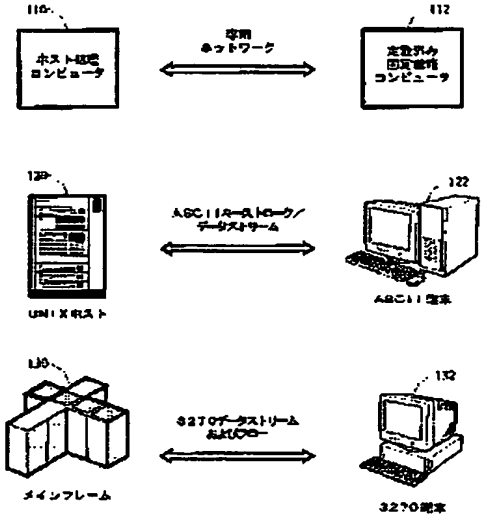
【図９】第３のシナリオのメッセージ伝送を示す流れ図である。

【図１０】図６のサービス・サーバのサービス要求の処理を示す流れ図である。

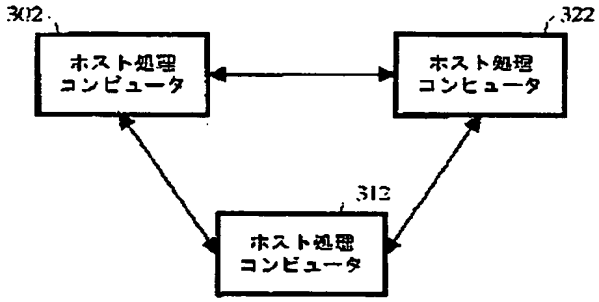
【図１１】図６のサービス・サーバのサービス要求の処理を示す流れ図である。

【図１２】図６のサービス・クライアントのサービス・サーバ・イベントの処理を示す流れ図である。

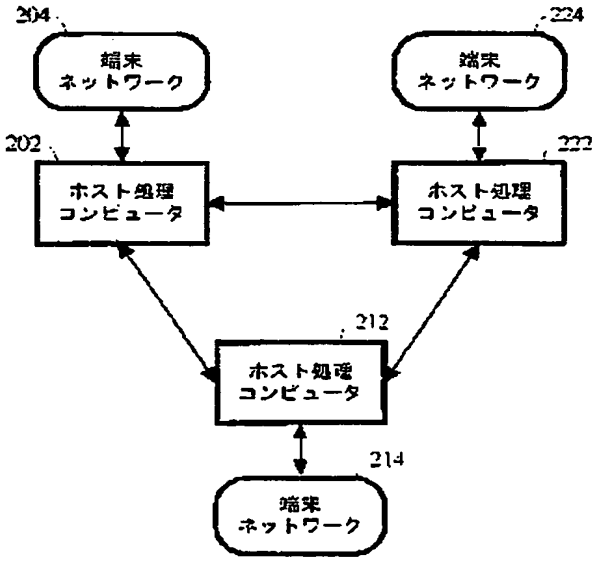
【図１】



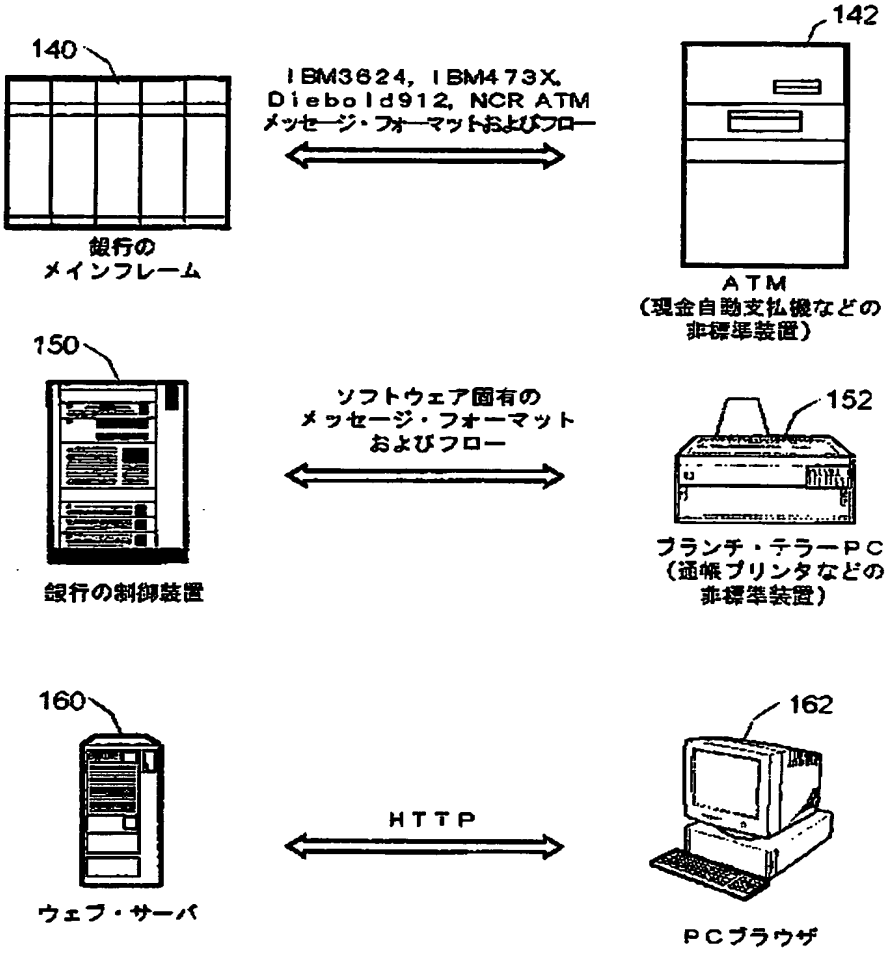
【図４】



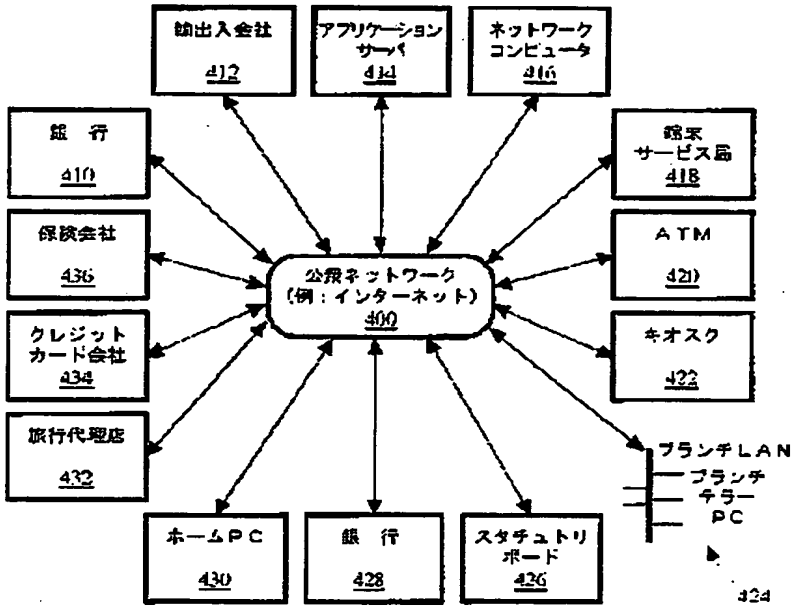
【図３】



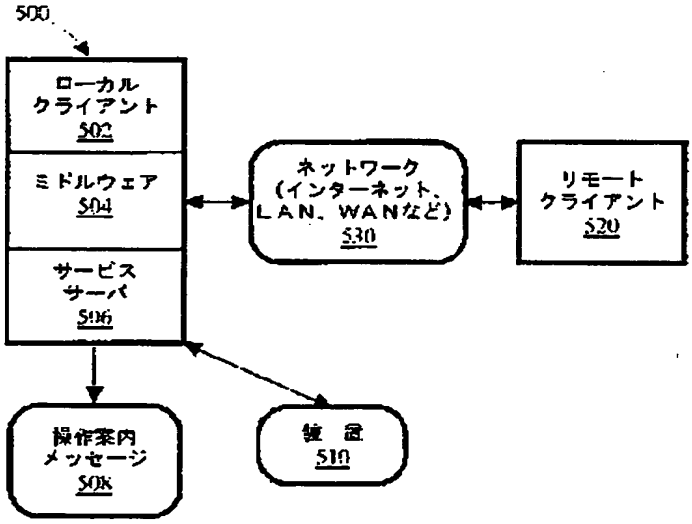
【図２】


140
IBM3624, IBM473X,
Diebold912, NCR ATM
メッセージ・フォーマットおよびフロー
142
銀行の
メインフレーム
ＡＴＭ
（現金自動支払機などの
非標準装置）
150
ソフトウェア固有の
メッセージ・フォーマット
およびフロー
152
銀行の制御装置
ブランチ・テラーＰＣ
（通帳プリンタなどの
非標準装置）
160
ＨＴＴＰ
162
ウェブ・サーバ
ＰＣブラウザ

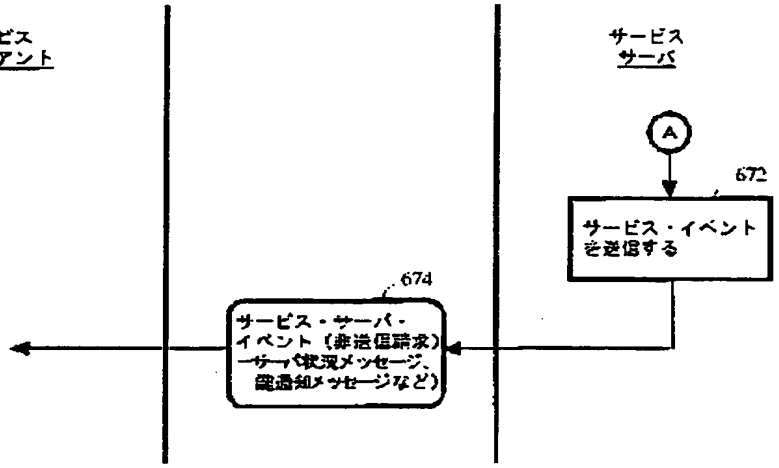
【図５】


出入金会社
412
アプリケーション
サーバ
414
ネットワーク
コンピュータ
416
銀　行
410
端末
サービス局
418
保険会社
436
ＡＴＭ
420
公衆ネットワーク
（例：インターネット）
400
クレジット
カード会社
434
キオスク
422
旅行代理店
432
ブランチＬＡＮ
ブランチ
テラー
ＰＣ
ホームＰＣ
430
銀　行
428
スタチュトリ
ボード
426
424

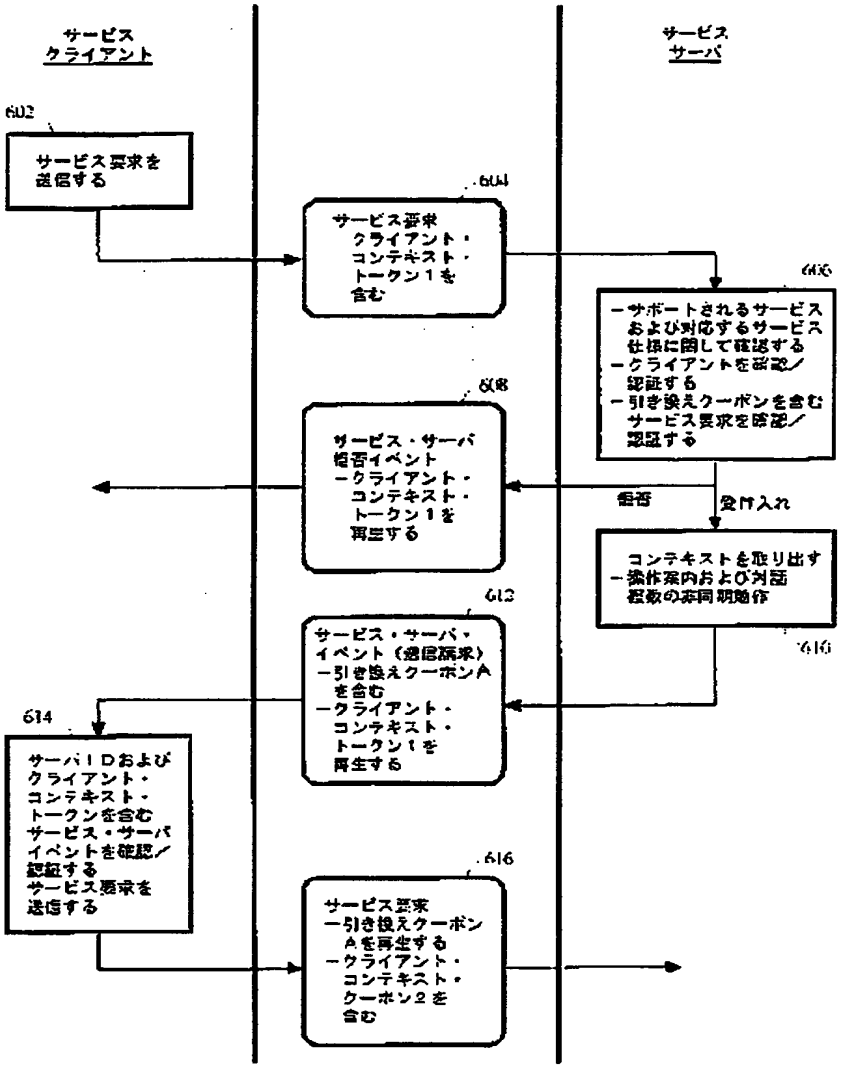
【図６】


500
ローカル
クライアント
502
ミドルウェア
504
サービス
サーバ
506
ネットワーク
（インターネット、
ＬＡＮ、ＷＡＮなど）
530
リモート
クライアント
520
操作案内
メッセージ
508
装　置
510

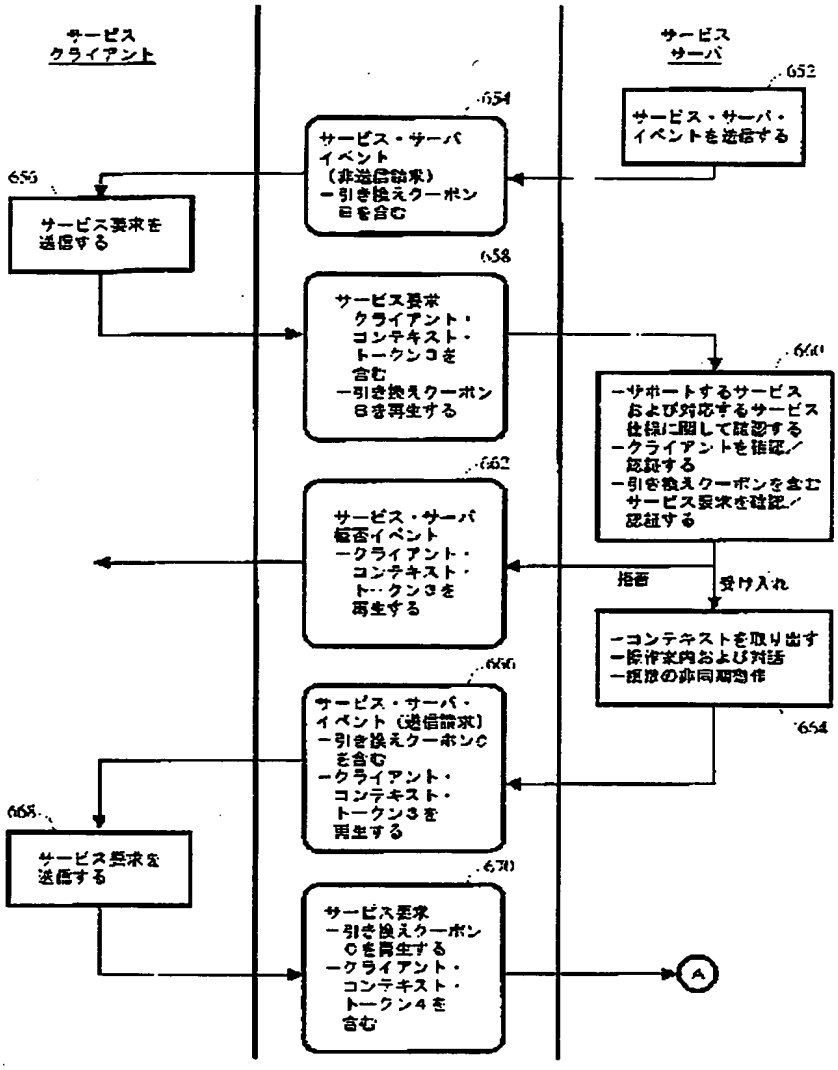
【図９】


サービス
クライアント
サービス
サーバ
A
672
サービス・イベント
を送信する
674
サービス・サーバ・
イベント（非送信請求）
－サーバ状況メッセージ、
認識メッセージなど）

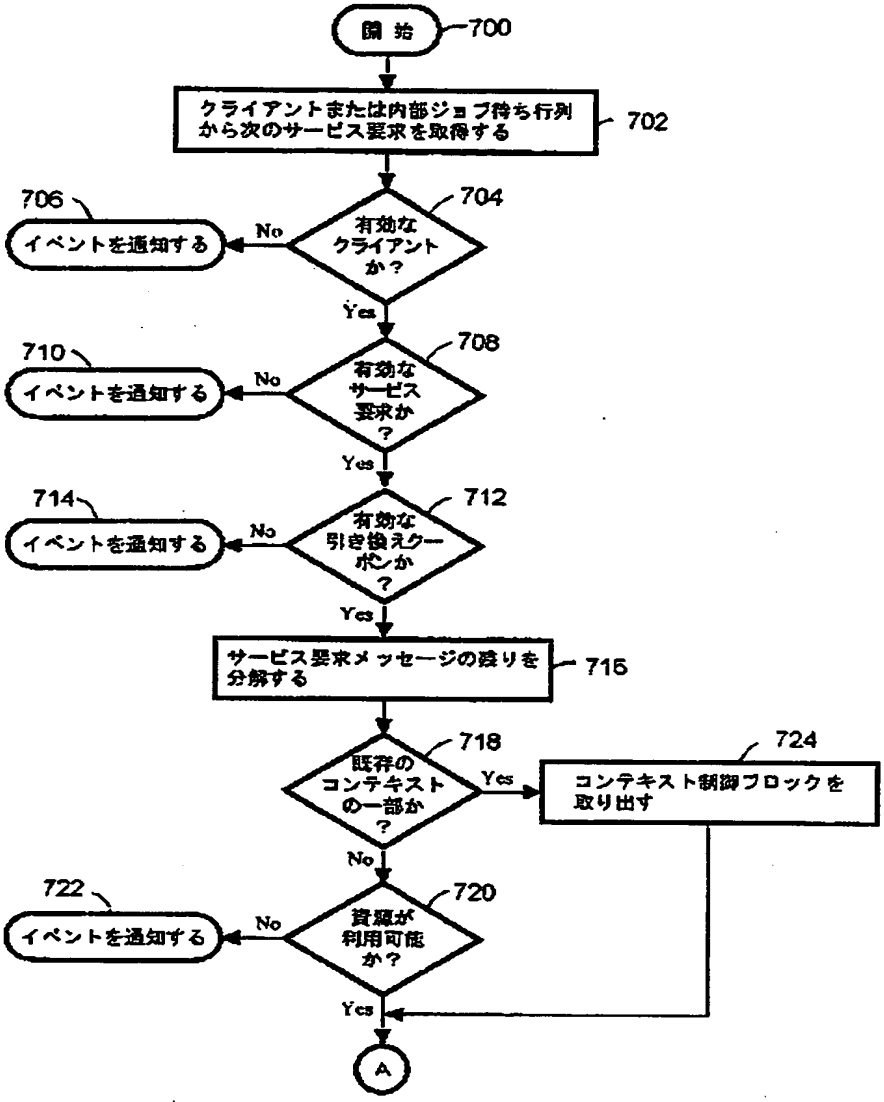
【図７】


サービス
クライアント
サービス
サーバ
602
サービス要求を
送信する
604
サービス要求
－クライアント・
コンテキスト・
トークン１を
含む
606
－サポートされるサービス
および対応するサービス
仕様に関して確認する
－クライアントを認識／
認証する
－引き換えクーポンを含む
サービス要求を確認／
認証する
608
サービス・サーバ
拒否イベント
－クライアント・
コンテキスト・
トークン１を
再生する
拒否
受け入れ
コンテキストを取り出す
－操作案内および対話
複数の非同期動作
616
612
サービス・サーバ・
イベント（通信開始）
－引き換えクーポンA
を含む
－クライアント・
コンテキスト・
トークン１を
再生する
614
サーバＩＤおよび
クライアント・
コンテキスト・
トークンを含む
サービス・サーバ
イベントを確認／
認証する
サービス要求を
送信する
616
サービス要求
－引き換えクーポン
Ａを再生する
－クライアント・
コンテキスト・
クーポン２を
含む

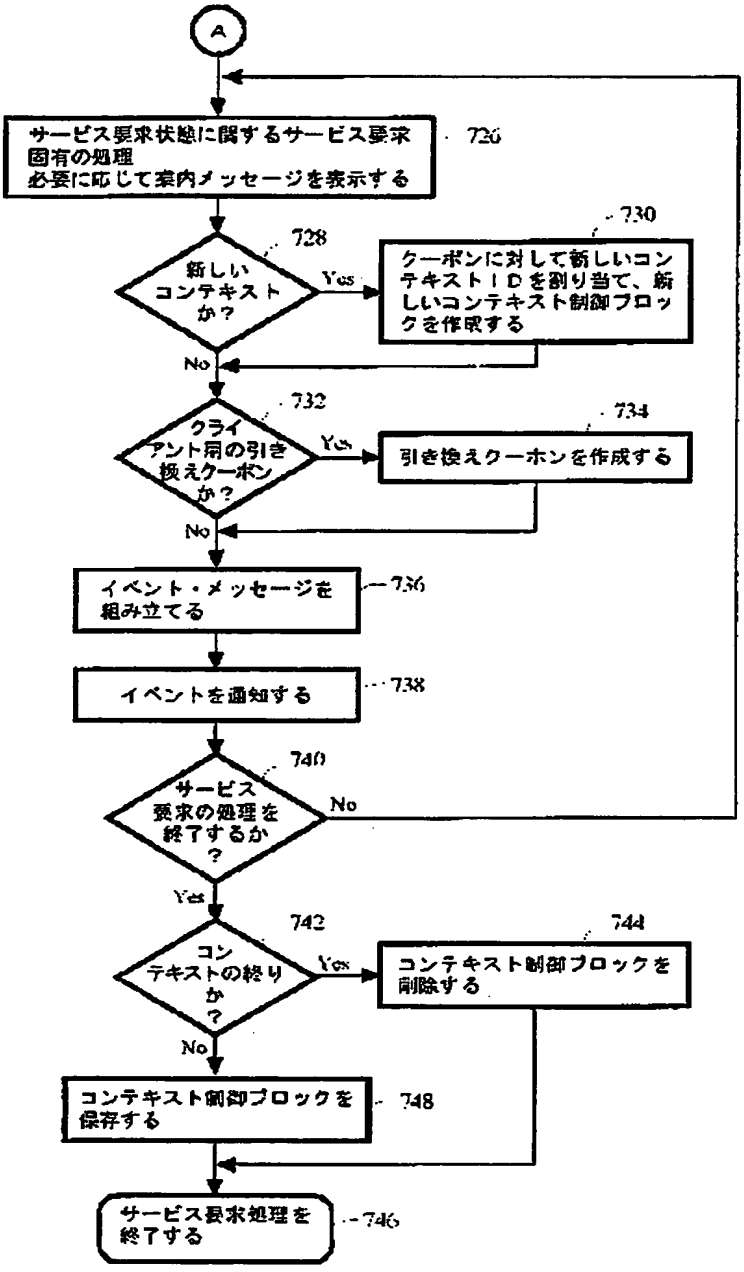
【図８】


サービス
クライアント
サービス
サーバ
652
サービス・サーバ・
イベントを送信する
654
サービス・サーバ
イベント
（非送信請求）
－引き換えクーポン
Ｂを含む
656
サービス要求を
送信する
658
サービス要求
クライアント・
コンテキスト・
トークン３を
含む
－引き換えクーポン
Ｂを再生する
660
－サポートするサービス
および対応するサービス
仕様に照して確認する
－クライアントを確認／
認証する
－引き換えクーポンを含む
サービス要求を確認／
認証する
662
サービス・サーバ
転否イベント
－クライアント・
コンテキスト・
トークン３を
再生する
拒否
受け入れ
－コンテキストを取り出す
－照会案内および対話
－複数の非同期動作
664
666
サービス・サーバ・
イベント（送信請求）
－引き換えクーポンＣ
を含む
－クライアント・
コンテキスト・
トークン３を
再生する
668
サービス要求を
送信する
670
サービス要求
－引き換えクーポン
Ｃを再生する
－クライアント・
コンテキスト・
トークン４を
含む
A

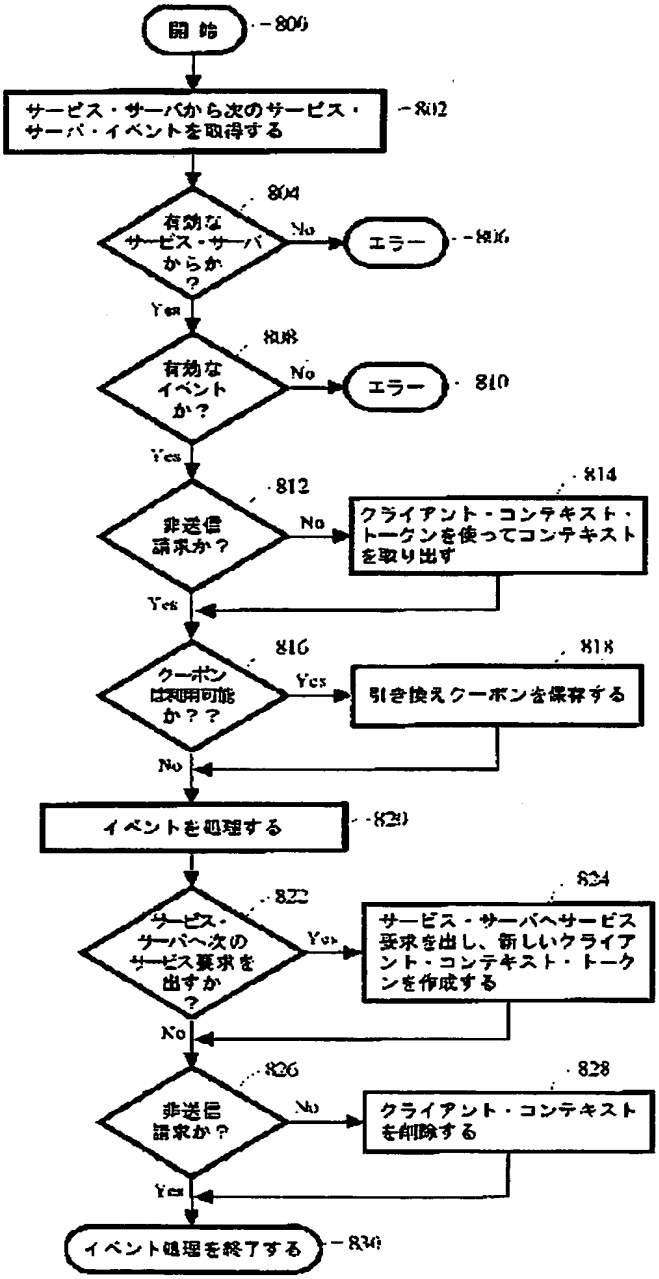
【図１０】


開始
700
クライアントまたは内部ジョブ待ち行列から次のサービス要求を取得する
702
有効なクライアントか？
704
No
イベントを通知する
706
Yes
有効なサービス要求か？
708
No
イベントを通知する
710
Yes
有効な引き換えクーポンか？
712
No
イベントを通知する
714
Yes
サービス要求メッセージの残りを分解する
715
既存のコンテキストの一部か？
718
Yes
コンテキスト制御ブロックを取り出す
724
No
資源が利用可能か？
720
No
イベントを通知する
722
Yes
A

【図１１】


A
サービス要求状態に関するサービス要求固有の処理
必要に応じて案内メッセージを表示する
726
728
新しいコンテキストか？
Yes
730
クーポンに対して新しいコンテキストＩＤを割り当て、新しいコンテキスト制御ブロックを作成する
No
732
クライアント用の引き換えクーポンか？
Yes
734
引き換えクーポンを作成する
No
イベント・メッセージを組み立てる
736
イベントを通知する
738
740
サービス要求の処理を終了するか？
No
Yes
742
コンテキストの終りか？
Yes
744
コンテキスト制御ブロックを削除する
No
コンテキスト制御ブロックを保存する
748
サービス要求処理を終了する
746

【図12】


開始
800
サービス・サーバから次のサービス・サーバ・イベントを取得する
802
有効なサービス・サーバからか？
804
No
エラー
806
Yes
有効なイベントか？
808
No
エラー
810
Yes
非送信請求か？
812
No
クライアント・コンテキスト・トークンを使ってコンテキストを取り出す
814
Yes
クーポンは利用可能か？？
816
Yes
引き換えクーポンを保存する
818
No
イベントを処理する
820
サービス・サーバへ次のサービス要求を出すか？
822
Yes
サービス・サーバへサービス要求を出し、新しいクライアント・コンテキスト・トークンを作成する
824
No
非送信請求か？
826
No
クライアント・コンテキストを削除する
828
Yes
イベント処理を終了する
830

フロントページの続き

(56)参考文献 国際公開97／23838（WO．Ａ１）
Goldstein. T.,"The Gateway Security Model in the Java Electronic Commerce Framework", Lecture Notes in Computer Science. Feb. 1997, No. 1318. p. 340－354

(58)調査した分野(Int.Cl.', ＤＢ名)
G06F 17/60 324
G06F 17/60 410
G06F 17/60 502
G06F 13/00 357
ＪＩＣＳＴファイル（ＪＯＩＳ）